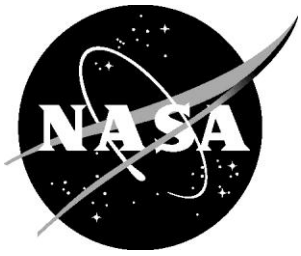
NASA/CR–2013-217801



Safety Sufficiency for NextGen

Assessment of Selected Existing Safety Methods, Tools, Processes, and Regulations

Xidong Xu, Mike L. Ulrey, John A. Brown, Jim Mast, and Mary B. Lapis
Boeing Research & Technology, Seattle, Washington

February 2013

NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NASA Aeronautics and Space Database and its public interface, the NASA Technical Report Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA Programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers, but having less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include organizing and publishing research results, distributing specialized research announcements and feeds, providing information desk and personal search support, and enabling data exchange services.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at *http://www.sti.nasa.gov*

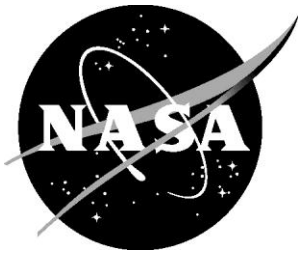
- E-mail your question to help@sti.nasa.gov

- Fax your question to the NASA STI Information Desk at 443-757-5803

- Phone the NASA STI Information Desk at 443-757-5802

- Write to:
  STI Information Desk
  NASA Center for AeroSpace Information
  7115 Standard Drive
  Hanover, MD 21076-1320

NASA/CR–2013-217801



Safety Sufficiency for NextGen

Assessment of Selected Existing Safety Methods, Tools, Processes, and Regulations

Xidong Xu, Mike L. Ulrey, John A. Brown, Jim Mast, and Mary B. Lapis
Boeing Research & Technology, Seattle, Washington

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

Prepared for Langley Research Center
under Contract NNL06AA04B/NNL12AB38T

February 2013

Acknowledgments

This contract work was awarded by NASA under Contract No. NNL06AA04B (Task Order No. NNL12AB38T). The NASA technical monitor for this task is Mr. C. Michael Holloway. We appreciate our Boeing colleagues, Mr. Keith Angus, Dr. Jeffery Musiak, and Mr. Paul Newton, for their contributions. We also benefited from the comments and suggestions made by another Boeing colleague, Ms. Monica Alcabin, when she reviewed an early version of this document. During the course of the work, we communicated with the following people and would like to thank them for meaningful discussions and providing references: Dr. Roland Weibel of the Massachusetts Institute of Technology (MIT), Mr. Eric Perrin of the European Organization for the Safety of Air Navigation (EUROCONTROL), Dr. Mariken Everdij of National Aerospace Laboratory (NLR) in the Netherlands, and Mr. Yimin Zhang of George Mason University.

Available from:

NASA Center for AeroSpace Information
7115 Standard Drive
Hanover, MD 21076-1320
443-757-5802

Table of Contents

Table of Figures

Table of Tables

Executive Summary

The Next Generation Air Transportation System (NextGen) is to transform the current US air transportation system in order to increase its capacity, efficiency, and reliability, as well as minimize its environmental impact. NextGen is a complex socio-technical system and, in many ways, it is expected to be more complex than the current system. While many NextGen elements (technologies, systems, and procedures) may increase safety, the expected increase in complexity may, under certain circumstances (e.g., automation failures), complicate safety situations. Yet, according to the Joint Planning and Development Office (JPDO), NextGen must be safer than today's system in managing the projected growth in air traffic volume. Therefore, it is vital to assess the safety impact of the NextGen elements in a rigorous and systematic way and to ensure that they do not compromise safety.

We first surveyed a number of major NextGen documents and databases including the JPDO Enterprise Architecture for the NextGen, JPDO NextGen Integrated Work Plan, the FAA NAS Enterprise Architecture, and the FAA NextGen Implementation Plan. We identified all of the NextGen elements in the form of Operational Improvements (OIs), Enablers, Research and Development (R&D) Activities, and Policy Issues.

Next, we outlined the overall hazard situation in NextGen. Several features of NextGen may contribute to the challenging hazard situation, including higher traffic density, higher levels of automation, more tightly-coupled operations, decentralized operations, and introduction of multiple elements within a short time. Following that, we performed a high-level hazard analysis associated with multiple elements in a particular OI known as OI-0349 (Automation Support for Separation Management), using our Socio-Technical Framework of Hazard Identification. Hazards were identified from the following factors and their interactions: humans, machines (both hardware and software), environment, as well as organizational factors and factors outside organizations. This was followed by a high-level analysis of hazards in a Fight Deck Interval Management for Spacing (FIM-S) scenario, which is part of the same OI. We illustrated how hazards can result from the highly dynamic complexity involved in that NextGen scenario, a situation that is not experienced in the current system.

Then we reviewed a selected but representative set of the existing safety methods, tools, processes, and regulations and analyzed whether they are sufficient to assess safety in the elements of that OI and ensure that safety will not be compromised. The results indicate the following:

- Overall, the existing methods and tools used in the United States do not appear to be sufficient because they do not allow full consideration of the dynamic complexity.
- The existing processes for safety certification and approval in this country are mostly not sufficient because they are conducted for individual components (e.g., aircraft and its systems, ground facilities, and air traffic procedures) separately, but not for the whole system associated with an OI.
- Similarly, corresponding regulations are not sufficient because they are imposed for the safety of individual components only, but not for the system of the relevant OI.

We also assessed the costs of the methods, tools, processes and regulations. The inadequate methods, tools, processes, and regulations might incur intolerably high costs in the long term, including costs of not meeting the required NextGen safety level. On the other hand, an adequate approach can also be costly because of the time and resources required for the

development and validation. However, the costs of an adequate approach should be weighed against the costs of an inadequate approach.

Based on the assessments, we make several recommendations, which we believe may lead to improvements. Specifically, there is a need for continuous innovation, including the development of new methods and tools, and improvement of the safety processes and regulations. An important part of this effort would be a more systematic review and assessment of the methods, tools, processes, and regulations associated with safety of Single European Sky ATM Research (SESAR). Some of the approaches and practices for SESAR safety could be adopted for ensuring NextGen safety as they face similar safety challenges.

1. Introduction

The Next Generation Air Transportation System (NextGen) is to transform the current US air transportation system in order to increase its capacity, efficiency, and reliability, as well as minimize its environmental impact. NextGen is a complex socio-technical system and, in many ways, it is expected to be more complex than the current system. While many NextGen elements (technologies, systems, and procedures) may increase safety, the expected increase in complexity may, under certain circumstances (e.g., automation failures), complicate the safety situation. Yet, according to the Joint Planning and Development Office (JPDO), NextGen must be safer than today's system in managing the projected growth in air traffic volume [1]. Therefore, it is vital to assess the safety impact of the NextGen elements in a rigorous and systematic way and to ensure that they do not compromise safety.

The scope of this work is to evaluate the hazards that are likely to arise during the implementation and deployment of NextGen systems, and assess whether existing safety methods, tools, processes, and regulations are sufficient to address adequately each issue or hazard. A hazard may be said to be "addressed adequately" if 1) a suitably high degree of confidence can be justifiably obtained that the issue or hazard will not result in a decrease in the safety of air transportation, and 2) the cost of obtaining the requisite degree of confidence is tolerable.

The objective of this work is to 1) identify proposed and planned NextGen elements (technologies, systems, and procedures), 2) assess their safety implications (for a number of these elements, this assessment includes a high-level hazard analysis that takes into consideration potential hardware, software, human, environmental, organizational, and other factors), 3) assess a selected but representative set of the existing tools, methods, procedures, and regulations in terms of whether they are sufficient to ensure that the current level of safety is not compromised, and whether they might incur intolerably high costs.

2. Identification of Planned and Proposed NextGen Technologies, Systems, and Procedures

In this section, we first outline the NextGen documents and databases we surveyed, followed by the identification of the NextGen elements, and the relationship among the elements found in various documents and databases.

2.1. NextGen Documents and Databases Surveyed

In order to identify the planned and proposed NextGen technologies, systems, and procedures, we surveyed a large number of NextGen documents and databases. Below are some examples:

- The JPDO Enterprise Architecture (EA) [2]
- The JPDO Integrated Work Plan (IWP) [3]
- Other JPDO documents such as NextGen Concept of Operations [1], Targeted NextGen Capabilities for 2025 [4], Net-Centric Operations Concept of Operations [5], and JPDO Trajectory-Based Operations (TBO) Study Team Report [6]
- The FAA National Airspace System Enterprise Architecture (NAS EA) [7]
- The FAA NextGen Implementation Plan (NGIP) 2012 [8]

- Other FAA documents such as the AVS Work Plan for NextGen 2012 [9], FAA 2009-2013 Flight Plan [10], 2011 National Aviation Research Plan [11], and National Airspace and Procedure Plan 2010 [12]

FAA AVS Work Plan for NextGen 2011 [9] summarizes the following four major NextGen documents and databases, which contain most of the JPDO and FAA planning elements activities:

- The JPDO EA is "the blueprint for NextGen…describes the segments, capabilities, operational activities, and identified relationships to the key target components of NextGen in the year 2025…The key difference between the JPDO EA and the FAA's NAS Enterprise Architecture is the JPDO EA has a broader scope and looks at the entire air transportation system, including operations and systems beyond the responsibilities of the FAA" [9, p. 27].
- The JPDO IWP "supports the collaborative planning and deliberation among partners and stakeholders to prioritize needs, establish commitments, coordinate efforts, and focus resources on the work needed to achieve NextGen. The IWP provides comprehensive information about the elemental operational improvements, enablers, development and research milestones, and policies that define the overall NextGen plan) [9, p. 29].
- The FAA NAS EA "aims to provide accurate and concise architecture information for NAS enterprise-level decision making. The NAS EA includes a comprehensive set of Operational Improvements (OIs)…also includes operational depictions and technology roadmaps of the FAA's plans" [9, p. 29].
- FAA NGIP "provides an overview of the FAA's ongoing transition to NextGen. The NGIP addresses results of the previous year's activities as well as the FAA's current and mid-term commitments (2012-2018)" [9, p. 29].

Another major difference between the JPDO and the FAA planning is in look-ahead time. According to the FAA AVS Work Plan for NextGen 2011, "JPDO develops the overall vision and far-term plan while FAA plans and implements the majority of NextGen's near-term (current through 2012) and mid-term (2012 through 2018) goals" [13, p. 27].

2.2. NextGen Elements

The JPDO IWP, the FAA NAS EA, and the FAA NGIP contain most (if not all) the NextGen elements. Within the JPDO IWP, there are five planning element types (see Figure 1, [14, p. 11] for the relationship among the element types):

- "Operational Improvement (OI): An OI describes the operational changes needed to achieve the concepts and capabilities identified in the ConOps and EA. It describes a specific stage in the transformation and the performance improvements expected at that point in time…
- Enabler: An Enabler describes a specific functional component needed to support one or more OIs or other Enablers. Enablers describe both materiel components such as communication, navigation, and surveillance systems; and non-materiel components such as procedures, algorithms, and standards…
- Development Activity: Development Activities describe development initiatives or demonstrations and the results and/or outputs needed to support other NextGen planning elements…

- Research Activity: Research Activities describe basic or applied research initiatives and the results and/or outputs needed to support other NextGen planning elements…
- Policy Issue: Many of the OIs and Enablers require policy changes to support their realization, particularly related to interoperability, standardization, and governance…" [15, pp. 2-3].

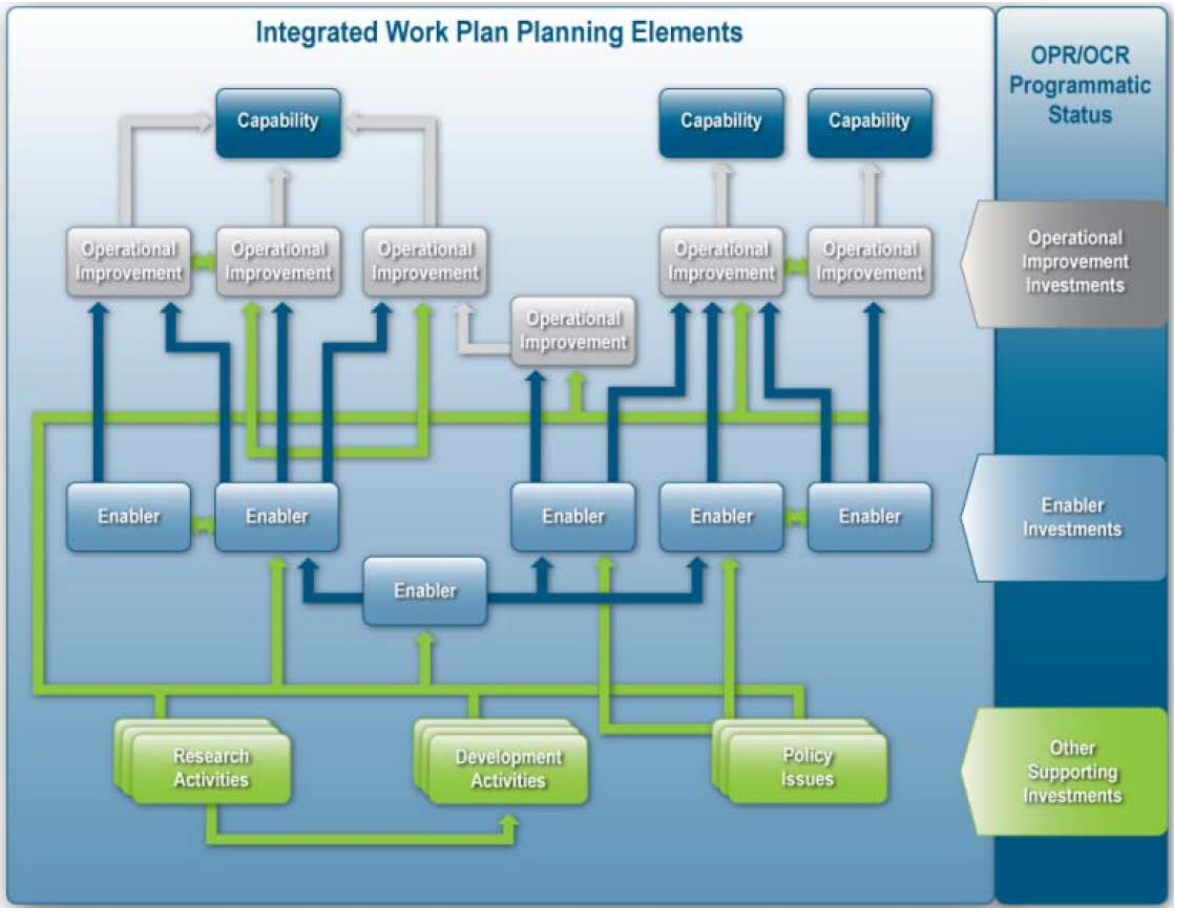


Figure 1. NextGen Elements

The FAA NAS EA contains several products:

- Service Roadmaps
- Operational Improvements
- Infrastructure Roadmaps
- Financial
- Architecture
- Requirements

The FAA NGIP, among other elements, also describes OIs, Supporting Common Services, Enablers, and the associated (FAA) Policies.

Based on the review of those documents and databases, we consider those elements in the IWP, NGIP, and NAS EA frameworks as the planned and proposed NextGen technologies,

systems, and procedures. This is justifiable because the technologies, systems, and procedures are either part of or embedded in those elements. The NextGen elements in the IWP (i.e., OIs, Enablers, Development Activities, Research Activities, and Policy Issues) can be found at the JPDO Joint Planning Environment (JPE) website (http://jpe.jpdo.gov/ee/request/page?id=1415). The FAA NAS EA products, including the OIs, can be found at FAA's NAS EA Portal (https://nasea.faa.gov/). The OIs, Supporting Common Services, Enablers, and the associated (FAA) Policies in the FAA NGIP can be found at its website (http://www.faa.gov/nextgen/implementation/plan/).

Figure 2 shows the relationship among the NextGen OIs in the various documents and databases. All of the OIs in the FAA NGIP are part of the FAA NAS EA OIs, which partly overlap with those in the JPDO's IWP.

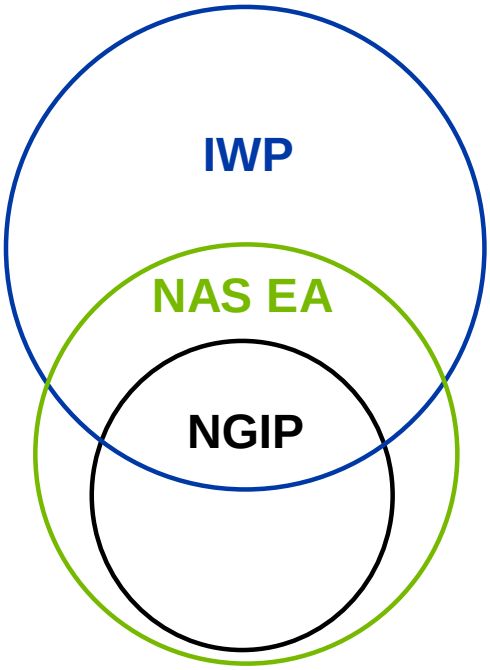


Figure 2. Relationship among NextGen OIs in IWP, NAS EA, and NGIP

3. Assessment of Safety Hazards

A hazard is defined by the FAA as a "condition, event, or circumstance that could lead to or contribute to an unplanned or undesired event" [16, p. 3- 4]. "Seldom does a single hazard cause an accident. More often, an accident occurs as the result of a sequence of causes termed initiating and contributory hazards" [16, p. 3- 4]. According to the FAA System Safety Handbook, there are hazards and contributory hazards (see Figure 3 [16, p. 3- 4]). Hence, unless otherwise noted, hazards will refer to a generic term, which includes both "hazards" and "contributory hazards."

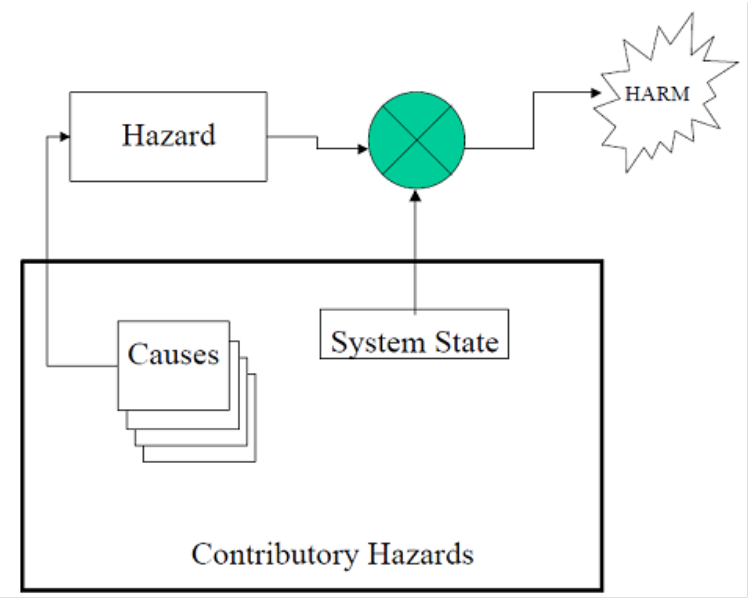


Figure 3. Accident Scenario Model

Hazard identification is an important part of safety risk management (SRM), which is required to be applied to any changes to the NAS, including the NextGen elements, to eliminate the risks or manage the risks below or at an acceptable level. As Figure 4 [17, p. 26] shows, hazard identification (along with the system description) is the prerequisite for other phases of the SRM process: risk analysis, assessment, and treatment [17], [18].

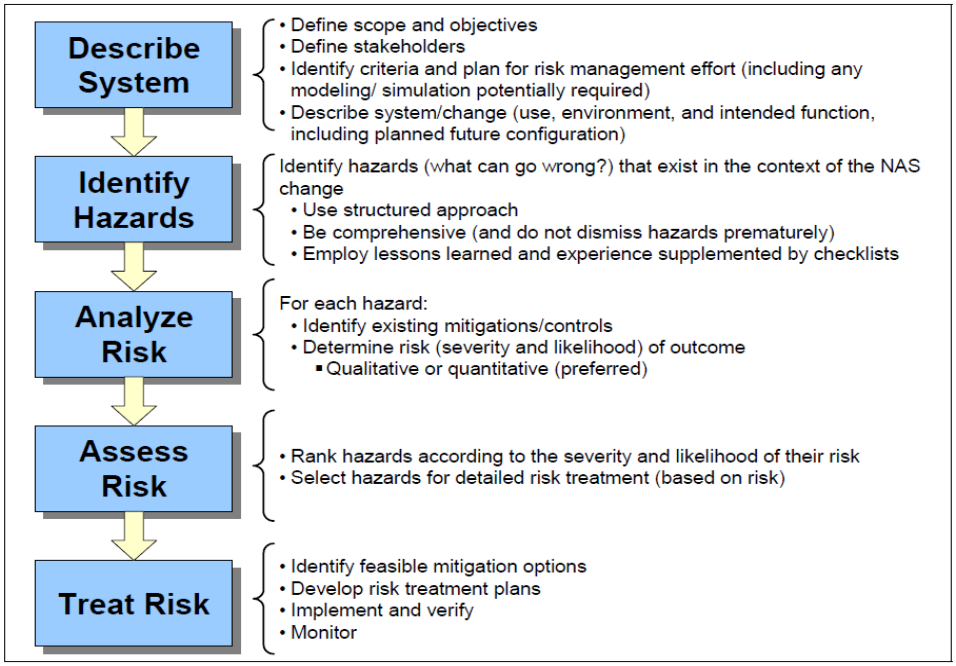


Figure 4. Typical Safety Risk Management Phases

The contemporary safety approach requires that hazards be identified from the multiple factors and components of a system and their interactions [17], [18], [19]. That is, hazards should be identified from liveware (i.e., human), hardware, software, and environmental factors and their interactions [20]. It is also critical to identify hazards from organizational factors and factors outside organizations [21].

In this section, we first outline the overall NextGen hazard situation. Next, we provide an analysis of hazards involved in OI-0349, which is then followed by an analysis of hazards involved in an OI-0349 scenario. The analysis in this section is a high-level analysis that represents only hazards resulting from a subset of all the possible factors and their interactions. A full-scale analysis that considers all the factors and all the interactions is beyond the scope of the current work.

3.1. Overall NextGen Hazard Situation

The air transportation system is a complex socio-technical system. Socio-technical systems are "systems in which people must actively and closely interact with technology to achieve production goals through delivery of services ..." [18, p. 4-1]. The air transportation system may also be thought of as a system of systems (SoS) and has the following characteristics, all of which contribute to hazards and risks [22]:

- Emergent properties
- Autonomous operations
- Interconnected constituents
- Ambiguous/changing boundaries
- Multiple contexts and influences
- Dynamic stakeholder relationships

The hazard situation in NextGen is, in many ways, more challenging than the current system for the following reasons:

- Higher traffic density than in the current system [1]
- Increased use of automation and automation at higher levels than in the current system [1]
- Operations that are more tightly coupled than in the current system [1], [23], [24], [25], [26]
- Decentralized operations vs. centralized operations in the current system [1], [26]
- Multiple new elements being or to be introduced simultaneously or within a shorter time than previously, making safety assessment and assurance a tremendous challenge [27].

All these features may contribute to increased complexity in NextGen, especially increase in dynamic complexity. Dynamic complexity refers to the "situations where cause and effect are subtle, and where the effects over time of interventions are not obvious" [28, p. 71]. Dynamic complexity is different from detail complexity. A system that simply contains a large number of components may have a large degree of detail complexity, but it is not necessarily dynamically complex, if the cause-effect relationship is straightforward and thus is easy to understand. In complex socio-technical systems such as the air transportation system, dynamic complexity results from the attributes of multiple factors or components in the system as well as their interactions. From the control-theoretical point of view [29], [30], the more complex a system is, the more unknowns there are in it, and thus the more difficult it is to understand how control

constraints (e.g., aircraft are not allowed to be closer to each other than the prescribed separation minima) might be violated and ultimately ensure they are not violated.

More specifically, a number of key factors in NextGen contribute to the increased complexity and thus present unique hazards to the safety:

- Machine factors—Compared to the current system, NextGen is a more software-intensive system [31] and such systems present unique safety challenges relative to hardware-intensive systems [30]. The complexity of software increases as the complexity of new avionic systems increases. Hardware reliability is also a concern [32]. As mentioned above, another critical machine factor is the more extensive use of automation at higher levels than today.
- Human factors—Among other human factors concerns are those associated with changes in automation. For example, there are four stages of automation in air traffic control (ATC): 1) information acquisition (such as display of aircraft position on radar screen for air traffic controllers), 2) information analysis (such as prediction of conflict between aircraft by computer), 3) decision selection (such as recommendation of conflict resolution by computer), and 4) action implementation (such as implementation of the recommended resolution by computer) (see Figure 5 [33]). Figure 5 also shows that the automation level in future systems will be higher at all the four stages than in the current systems, in particular at the two latter stages (decision selection and action implementation). Changes in automation will inevitably result in role changes for the operational personnel. The changed roles may significantly alter their workload and situation awareness, and lead to new types of human errors.
- Environmental factors—In particular, weather predictability issues may have hazardous impacts especially on Trajectory-Based Operations (TBO). TBO is reliant on the predictability of weather, and the uncertainty of the weather shortens the time horizon of predictability. This has implications for safety. For example, aircraft could be closer than they should be because of the incorrect weather prediction.
- Organizational and factors beyond organizations—R&D efforts to support the implementation of NextGen capabilities are complex [27]. This complexity may potentially impact the safety level of NextGen. Issues and gaps in safety-related methods, processes, regulations, including rules and standards, are numerous, a topic that will be further discussed in section 4 of this document. Other safety-related factors include global interoperability issues [34], [35], availability of budget to support the development and implementation of NextGen elements [36], and lack of qualified air traffic controllers at critical ATC facilities [37].

To a certain extent, the above outline of the unique features of the multiple factors (human, machine, environmental, organizational, and other factors) has implied their possible interactions. Section 3.2 describes the results of a high-level hazard analysis for a NextGen OI. While all the features outlined above are applicable to that OI, section 3.2 describes in more detail the interactions among the multiple factors involved in that OI.

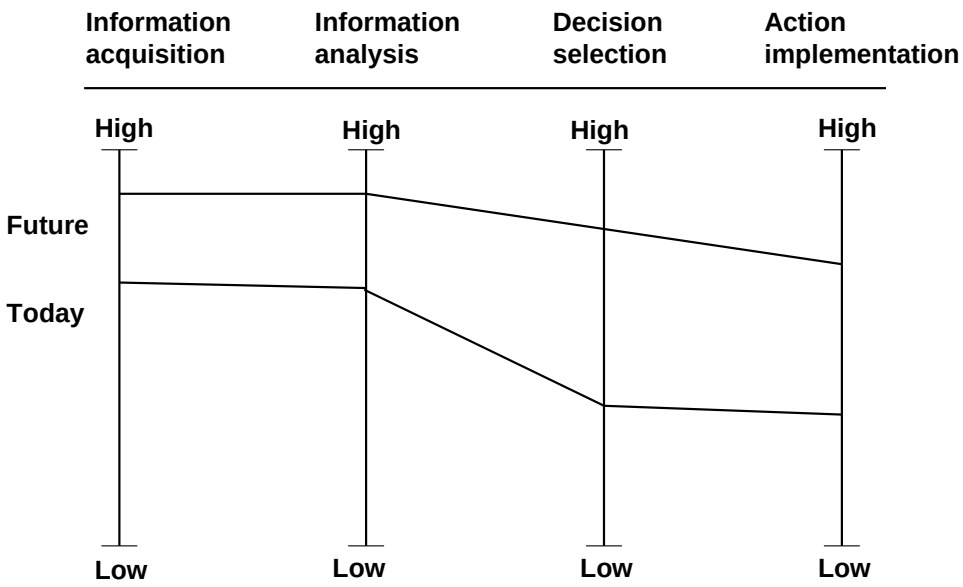


Figure 5. Today and Future Automation Levels of ATC Systems
(@ 2000 IEEE. Derivation of original figure used with permission, from Figure 2 in [33, p. 288]).

3.2. Hazards in OI-0349 (Automation Support for Separation Management)

Our criterion for choosing a NextGen OI for the hazard analysis is that it, along with its constituent elements, should be representative of NextGen operations. We chose OI-0349 (Automation Support for Separation Management) to perform a high-level hazard analysis because it includes the key features of NextGen: high-level automation, tightly-coupled and decentralized operations, dynamic complexity, high traffic density, and many new elements to be introduced within a short time. OI-0349 is described by the JPDO IWP as follows:

> The ANSP automation provides the controller with tools to manage aircraft separation in a mixed navigation and wake performance environment. Aircraft with various operating and performance characteristics will be operating within the same volume of airspace. Controllers will use ANSP automation enhancements to provide situational awareness of aircraft with differing performance capabilities (e.g., delegated self-separation maneuvers, equipped vs. non-equipped aircraft, RNAV, RNP, and trajectory flight data management). For example in performance-based navigation, RNAV/RNP routes may be spaced closer than the normally required separation for the sector area. The standard system conflict alert and conflict probe for the designated area account for this reduced spacing. These enhancements enable ANSP to manage the anticipated increase in complexity and volume of air traffic. [3, http://jpe.jpdo.gov/ee/request/elementForm?id=1020209].

Our Socio-Technical Framework of Hazard Analysis [35] was used to guide the analysis, because it takes into consideration potential hardware, software, human, and environmental factors, as well as influences from organizational factors and factors beyond organizations (see Figure 6, adapted from Figure 4 in [35, p. 8B4-7].

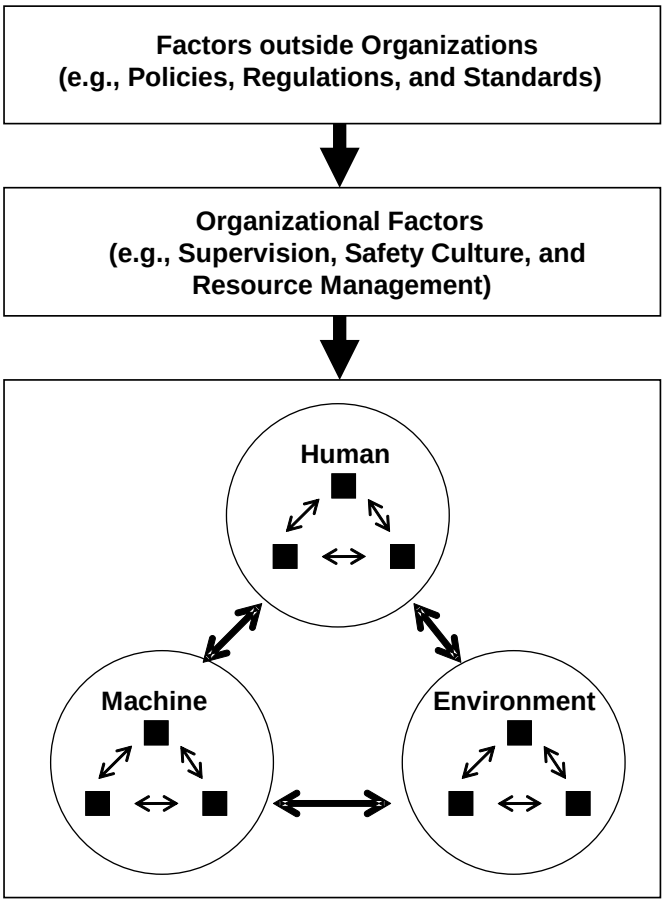


Figure 6. Major Components in the Socio-Technical Framework of Hazard Identification

Because OI-0349 is still in the concept phase, the hazard analysis is basically a preliminary hazard analysis [35], [38]. This early hazard analysis is in alignment with JPDO's position, "The incorporation of safety risk management into concept planning activities is consistent with the National Safety Management System (SMS) standard developed by the Safety Working Group (WG)" [39, p. 3].

An important question concerns the relationship among hazards already existing in the current system and new hazards that may arise in NextGen. That is, should we only examine hazards unique to the NextGen elements (OIs, Enablers, Development Activities, Research Activities, and Policy Issues)? Or should we also examine the hazards associated with the remaining elements of the current system? In this study, we included some hazards that are common to both the current system and NextGen (e.g., weather). Further, a latent hazard suppressed in the current system could manifest itself when interacting with the new (NextGen) elements [21]. A major source of latent hazards is mixed equipage. In this study, we also included some examples of how hazards can emerge as a result of interactions among some equipment that exists in the current system and will remain in NextGen and some new equipment in NextGen. Figure 7 (adapted from Figure 5 in [35, p. 8B4-8]) schematically shows the relationship among hazards in the current system and those in the NextGen.

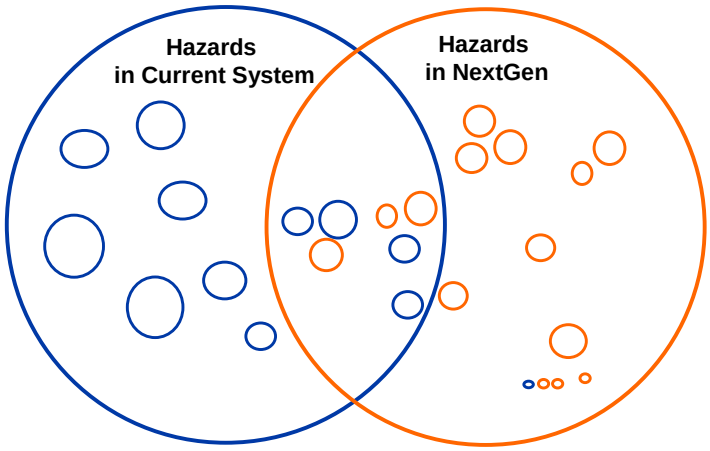


Figure 7. Schematic Relationship among Hazards in the Current System and NextGen.

The steps we undertook in the hazard analysis are described below in chronological order:

- Step 1. The description of the OI was extracted from a JPDO IWP website http://jpe.jpdo.gov/ee/request/elementForm?id=1020209.
- Step 2. The timetable for the OI was found at a JPDO IWP website http://jpe.jpdo.gov/ee/request/page?id=1415. The information available includes descriptions of the supporting Enablers and associated Policy Issues.
- Step 3. The same website provided linkage to the Enablers that support the specific Enablers defined for the OI, as well as the supporting R&D activities, and the associated Policy Issues (see Appendix B for the descriptions of these elements). This information was also extracted.
- Step 4. A diagram that illustrates the relationships among the OI, the supporting Enablers, R&D Activities, and Policy Issues was constructed (see Appendix C).
- Step 5. Hazards were identified as a result of the interactions among human, environmental, and machine (both hardware and software) factors, as well as of the influences from organizational and extra-organizational factors such as regulations and international interoperability.

The main hazards in this OI are loss of safe separation between aircraft, and between aircraft and the terrain. Contributory hazards may result from multiple types of interactions: machine-machine, machine-environment, human-machine, human-human, environment-environment, human-environment, as well as from organizational influences and influences from factors outside organizations. The next eight subsections describe in more detail the results of the hazard analysis by type of interaction and influence.

3.2.1. Machine-Machine (both Hardware and Software) Interaction

- Inter-dependency among this OI and ENs, and among ENs (e.g., EN-0039, EN-0212, EN-0016, EN-0035, EN-1231, EN-1271) make reliability of the system quite vulnerable
- Further, reliability is necessary but not sufficient for system safety. For example, software can reliably do the wrong thing.
- Automation may not be reliably aware of, and tracking, all the aircraft for which the controller has responsibility (EN-0035)
- Automation may not be reliably aware of aircraft performance characteristics, including any degraded capability (EN-0035)

- Automation may not be able to reliably track both delegation of separation responsibility and whether the aircraft remains within the limits delegated (EN-0035)
- Interactions between Unmanned Aircraft System (UAS) and regular aircraft presents unique hazards (EN-0039)

3.2.2. Machine-Environment Interaction

The factors from the following Enablers may impact the accuracy of the weather forecast and consolidation:

- EN-2680 Methodologies and Algorithms for Weather Assimilation into Decision-Making (supported by or related to R-1230, R-2112, R-2114, PI-0086, and PI-0087)
    - This Enabler depends on research, which may, or may not, yield useful results.
    - Models (e.g., wake forecast) and weather forecasts may not be accurate enough to yield useful information on the required scales. Automated algorithms for extracting relevant weather phenomena or conditions may not exist. Manual extracting may not be feasible.
- EN-2010 NextGen 4D Weather Cube Information – Manual SAS Selection (supported by R-2112 and PI-0088)
    - Lack of observations in some areas (e.g., over oceans)
    - Weather satellites are decaying
    - Combining multiple forecasts into a Single Authoritative Source may have the tendency to increase the probability of missing extreme events
    - Does an incentive exist for the holders of the best data and highest resolution models to share with everyone?
    - Climate change may drive the physics of some forecast models past current valid ranges
- EN-2080 Network-Enabled User-Defined Weather Information Request Function (supported by R-2112)
    - Requires predefined weather request or exhaustive search and specification language to cover all possible requests
- EN-2060 Aviation Weather Information System – Network-enable Existing Systems (related to or supported by PI-0086, PI-0087, and PI-0088)
    - Will this be implemented over the ocean?
    - Precipitous decline in space observation systems
    - Huge volume of data
    - Differing goals of sensor participants (interest in small scale vs. large scale phenomena)
    - Proper metadata needs to exist alongside measurements
    - Quality control of data, sensors (accuracy and calibration) and metadata
- EN-2410 Weather Forecasts – Consolidated Convective Storm (also applies to EN-2420, EN-2430, EN-2440, EN-2450):
    - Dense enough data observations?
    - Sufficient resolution of forecast models?
    - Forecast accuracy varies with conditions and time of year
        - Forecasts for periods of benign weather will be more accurate for longer periods of time
        - Forecasts for periods of unstable weather (e.g., highly convective periods) will only be accurate for shorter periods of time

- EN-2430 Weather Forecasts - Consolidated Turbulence
    - Data from observations or reports? Objectivity is required
    - Need to properly translate to different aircraft sizes
- Issues can arise from interactions among UAS and the above elements (EN-0039)
- Inaccurate weather forecast and consolidation (e.g., wind speed and direction, air temperature, severe weather, and wake turbulence) may impact automation's prediction of aircraft positions [40].

3.2.3. Human-Machine Interaction

- Human factors issues due to high-level automation (EN-0035)
    - Loss of situation awareness
    - False alarms and misses [41], [42]
    - Sub-optimal distribution of workload (in normal vs. abnormal situations)
    - Skill degradation that only becomes apparent when controllers need to take over control of traffic manually. Same applies to pilots in highly automated aircraft
- Human factors issues due to mixed equipage (including UAS vs. regular aircraft) (EN-0035; EN-0039)
    - Mixed equipage and aircraft may increase workload and vulnerability to error.
    - Research has shown that operations of aircraft with mixed equipage (with and without data link) are feasible within the same airspace as long as the number of aircraft not equipped with data link is within a limit, but controller workload level may be unacceptable if the limit is exceeded [43].
- Human factors issues may arise if there is incompatibility or inconsistency among the software, for example, two separate but incompatible collision alerting systems, one on the ground and one in the cockpit. Software usability is another interaction challenge, for example, GUI (Graphic User Interface) associated with high-level automation.
- Oscillations and instability of an aircraft or even a traffic stream may be caused by factors such as automation failures, communication delays, delays in human decision and responses. The next section (section 3.3) illustrates this type of problems in an OI-0349 scenario.

3.2.4. Human-Human Interaction

- "NextGen operational concepts will require more effective and efficient communication and collaboration among pilots, controllers, dispatch, and maintenance personnel, especially during off-nominal events" [44, p. 27].
    - Loss of team situation awareness (e.g., due to using data link and electronic flight strips)
    - Insufficient Crew Resource Management (CRM) practice among flight crew members, flight crew members and controllers, and flight crew members and other operator resources such as dispatchers and maintenance personnel

3.2.5. Environment-Environment Interaction

A number of elements are relevant to this category of interaction (EN-2680, EN-2010, EN-2080, EN-2060, EN-2410, EN-2420, EN-2430, EN-2440, and EN-2450):

- The impact of weather prediction inaccuracy may be greater and less tolerable when the aircraft are in close proximity with the terrain.
- The impact of weather prediction inaccuracy might be greater in the ATM environment with denser traffic.

3.2.6. Human-Environment Interaction

Two elements are relevant to this category of interaction (EN-0035 and EN-2680):

- In the NextGen air traffic environment, there might be more communication delays using the data link than using voice for communication.
- Human performance may be impacted by machine-environment interactions (through human-machine interactions). For example, weather can impact automation's accuracy in predicting aircraft's trajectories, which in turn may impact human operators' behavior when they interact with automation.

3.2.7. Influences from Organizational Factors

EN-0035 is relevant to this category:

- "Recent changes to the Operational Error program and the Air Traffic Safety Action Program (ATSAP) program are aimed at establishing a nonpunitive safety reporting program and are a positive first step towards changing the culture and establishing a more collaborative relationship with controllers" [45, p. 12]. However, the implications of the changes for safety are not fully understood.
- People may not be able to report unsafe behaviors due to low transparency in high-level automation.
- There might be personnel selection and training issues. Controllers and pilots may not have all the required Knowledge, Abilities, and Skills (KAS) in the high-level automation environment, although there is evidence that the KAS of the current controllers are sufficient for the job with high-level automation.

3.2.8. Influences from Factors outside Organizations

- Inadequate R&D (Research & Development) methods and incorrect results such as wrong results regarding crew behaviors in the event of automation failures (e.g., EN-0035).
- Inadequate policies regarding the role of humans and automation (e.g., PI-0006).
- Gaps in regulations and standards such as ambiguous traffic rules and separation minima in the event of automation failures; ambiguous regulation on how much spacing is safe between aircraft with delegated separation (e.g., EN-0035) and lack of standards and regulations with respect to integration of UASs into the NAS (e.g., EN-0039 and R-1190).
- Global harmonization issues (e.g., PI-0086).
- Inadequate safety methods, tools, processes, and regulations are also a major hazard to the required safety level of NextGen (this will be more fully addressed in the next section (section 4).

It should be noted that elements from other OIs may contribute to the hazard situation in this OI. For example, factors in OI-0320 Initial Surface Traffic Management, OI-0321 Enhanced Surface Traffic Operations, and OI-0322 Low Visibility Surface Operations may impact the hazard situation in OI-0349, although the former are not included as elements of the latter. Likewise, the elements in this OI (0349) can also impact the safety of other OIs. The complex interactions among them may even have implications for the safety of the entire NextGen.

3.3. Hazards in a Scenario of OI-0349

While all the factors and their interactions described in subsections 3.1 and 3.2 are also applicable to an OI-0349 scenario whose hazards are analyzed in this subsection, the purpose of this analysis is to illustrate, at a high level, how some potential types of dynamic complexity involved in a highly automated operation can contribute to the loss of safe separation between aircraft and between aircraft and the terrain. These are the main hazards in this OI.

Figure 8 illustrates a scenario in OI-0349. The type of operation selected for the assessment is Flight Deck Interval Management – Spacing. A more comprehensive description of both simple and complex versions of the scenario is included in Appendix C. Figure 8 shows the complex version. This scenario is a decentralized operation, in which the flight crew of each trailing aircraft, enabled by automation in the aircraft, is responsible for achieving and then maintaining 90-sec spacing (a controller-selected parameter) from the target aircraft immediately preceding it in the flow. The air traffic controller, also equipped with automation, has the final responsibility for the safe separation between aircraft in the traffic string, and the controller-assigned spacing time or distance for which the flight crew is responsible has a buffer that provides for any necessary controller intervention to prevent loss of separation.

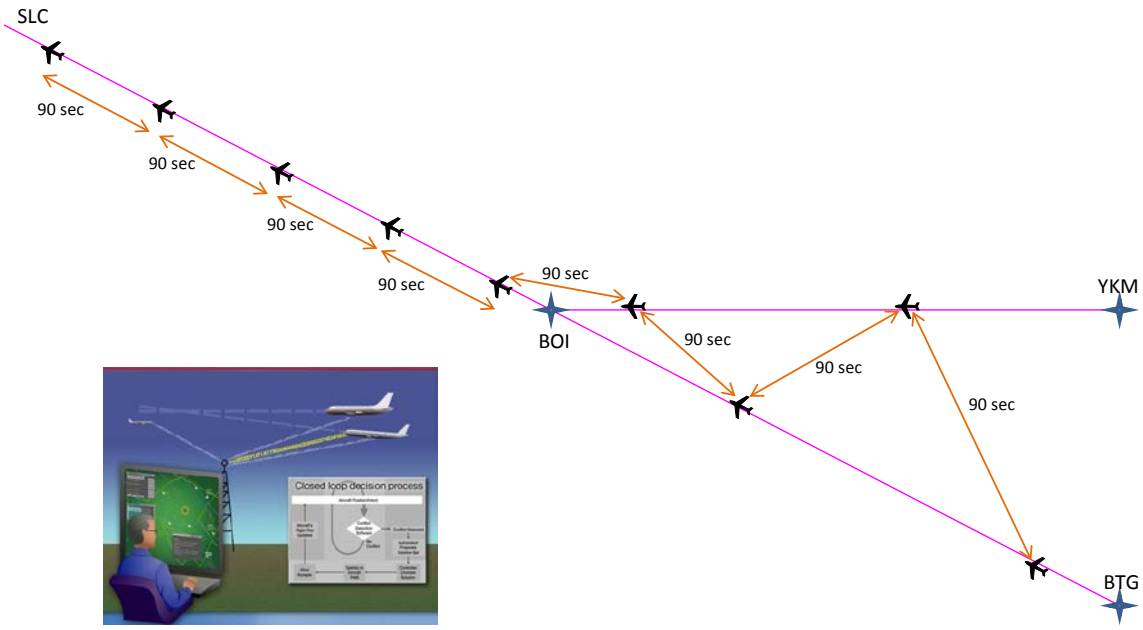


Figure 8. Scenario of Fight Deck Interval Management for Spacing (FIM-S)

Although the algorithm responsible for providing the flight crew with speed guidance for the FIM-S task is designed to minimize spacing instability, occasionally perturbations may occur (e.g., experienced wind and/or temperature values are significantly different from those used in FIM-S system predictions), perhaps exacerbated by an undetected system failure, and may cause spacing inaccuracy. In the scenario, spacing within one pair of aircraft close to the head of the flow reduces rapidly. Such inaccuracies would normally be detected by the FIM-S system, leading to changes in speed guidance and making the flight crew aware by using the FIM-S specific symbols on the cockpit display of traffic information (CDTI) as they monitor their spacing from the preceding aircraft. Because the flight crew has been removed from the speed control loop by the automation's functionality, and because the flight deck automation was reliable prior

to the problem, the flight crew has developed automation complacency, and thus fails to detect the inaccurate spacing, allowing the spacing between the two aircraft to become too close.

Similar to the flight deck automation, the ground automation can normally detect the spacing reduction, but may occasionally fail to do so. Yet, the controller is supposed to assure separation in the case of both airborne and ground automation problems. But similar to the flight crew, due to his/her complacency developed in the period of reliable automation, the controller fails to monitor or detect the problem. In the worst case, this situation may result in collision, but it is more likely the controller will eventually detect the loss of separation, and issue a speed reduction instruction that exceeds the capabilities of the FIM-S algorithm in the next aircraft in the flow to compensate effectively. Such an event could cause oscillation of the traffic in the string in the form of cyclic variation in longitudinal spacing as each aircraft, perhaps through flight crew or controller intervention in the FIM-S function, first reacts to rapidly reducing spacing, overcompensates, and then uses excessive speed to regain the assigned spacing value. This kind of oscillation is a typical result of dynamic complexity and may cause the loss of safe separation between aircraft and between aircraft and the terrain.

Further, because of the higher traffic density and the more tightly coupled operations in NextGen than in the current system, this hazardous situation may have a more severe ramification or impact along the traffic stream than it would in the current system. Other factors such as lack of standards for spacing, inappropriate training and safety culture, and global interoperability issues may contribute to the hazards in this scenario. It is obvious that the complexity in the entire OI-0349 will be greater than what is illustrated in this scenario as the latter is only part of the former.

4. Assessment of Selected Existing Safety Methods, Tools, Processes, and Regulations

For the safety hazards or issues identified in the above section, we assessed whether a selected but representative set of the existing safety methods, tools, processes, and regulations are sufficient to provide a suitably high degree of justifiable confidence that the issue will not result in a decrease in the safety of air transportation. The assessment was performed in the following six steps:

- Step 1. Defined safety methods, tools, processes, and regulations
- Step 2. Understood the relationship among them
- Step 3. Defined the scope of the existing safety methods, tools, processes, and regulations
- Step 4. Reviewed the existing methods, tools, processes, and regulations
- Step 5. Assessed the sufficiency of those methods, tools, processes, and regulations for NextGen safety
- Step 6. Assessed the costs of those methods, tools, processes, and regulations

In the following six subsections, we describe the results of each of the six steps.

4.1. Definitions of Safety Methods, Tools, Processes, and Regulations

Safety methods are defined in this study as techniques primarily used for hazard identification, risk analysis, risk assessment, and risk treatment. In this document, the two terms

(methods and techniques) are used inter-changeably. Safety tools refer to computer programs that help to implement methods. For example, fault tree analysis is a method (or technique). The various commercial and free software packages that help in conducting fault tree analysis are tools. Safety processes here primarily refer to those for safety risk management (SRM), safety approval, and certification. Note there are other safety-related processes such as those for certification of airmen, credentialing of air traffic controllers, and configuration management for ground-based equipment, but our emphasis is on SRM, certification and approval processes especially air traffic approval, aircraft certification, and operator certification, which are the core safety processes in the air transportation system. Finally, safety regulations in this study are government- or industry-imposed safety requirements or standards that must be met by a system.

4.2. Relationship among Safety Methods, Tools, Processes, and Regulations

Figure 9 illustrates the relationship among safety methods, tools, processes, and regulations. The diagram adopts a control-theoretical view of the relationship [29]. For any new system such as airborne equipment and ground-based facilities or procedures such as ATC procedures that have safety implications, there are two safety-related processes. The first is the SRM process; that is, safety experts and operational personnel use various methods and tools to perform SRM (description of system, hazard identification, risk analysis, risk assessment, and risk treatment) such that risk level (after risk treatment if this is needed) is at or below the acceptable level. This acceptable risk level would come from government- or industry-imposed regulations (standards or requirements). Aircraft certification, operator certification, and air traffic approval all take a risk-based approach to safety. They all have SRM processes in one form or another [17], [46], although a (better) system safety approach is desired [47], [48].

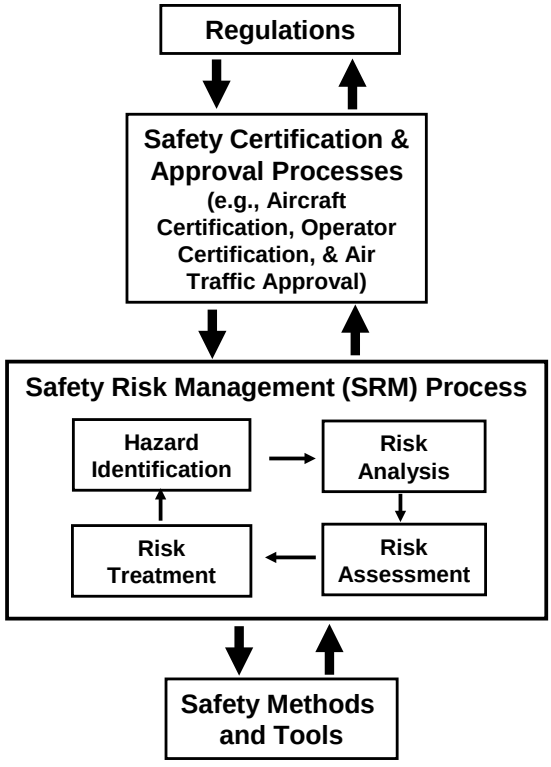


Figure 9. Schematic Relationship among Safety Methods, Tools, Processes, and Regulations

The second safety-related process is the safety certification or approval process. For example, the FAA would approve or certify a new system or procedure as adequately safe for deployment or implementation based on the appropriate standards or requirements. The various downward arrows in Figure 9 indicate control mechanisms. For example, regulations govern how safety certification and approval should be conducted and what methods should be used. The upward arrows in Figure 9 show the feedback mechanisms. For example, the results of SRM and the safety certification and approval processes would inform whether the existing regulations are appropriate.

4.3. Scope of Existing Safety Methods, Tools, Processes, and Regulations

The primary emphasis of our assessment is on the methods, tools, processes, and regulations that are actually in use or in place for the current US air transportation system. The secondary emphasis is on those that are the subject of ongoing consideration or being proposed for future use in the United States. These are typically based on the actual or perceived gaps in the current methods, tools, processes, and regulations, but which have not yet been used or put in place for the US system. Examples of those are FAA's ongoing methods and those proposed in conference papers. Those associated with Single European Sky ATM Research (SESAR) (mainly those as part of, or related to, joint U.S.-Europe programs or efforts) are also reviewed but at a higher level than for the US counterparts and are granted tertiary emphasis. Table 1 is a summary of primary, secondary, and tertiary emphasis.

Table 1. Emphasis of Assessment

	United States	**Europe**
In use or in place	Primary Emphasis	Tertiary Emphasis
Ongoing or proposed	Secondary Emphasis	Tertiary Emphasis

4.4. Existing Safety Methods, Tools, Processes, and Regulations

4.4.1. Existing Safety Methods and Tools

We first reviewed the traditional safety methods, which were mostly developed for SRM for relatively small and simple systems compared to large and complex socio-technical systems. Following that, we reviewed relatively new methods, which have been developed for handling larger and more complex socio-technical systems typically experiencing multiple and complex changes. Also reviewed were methods that have been used or developed specifically for assessing NextGen safety. The current processes for SRM, safety certification and approvals, along with their respective regulations in the United States were also identified. It needs to be pointed out that while we do not claim that our review is exhaustive, we believe it is representative, covering some major methods, tools, processes, and regulations, especially those used or in place in the United States.

For the traditional methods, we reviewed the following representative documents:

- Ericson [49) – *Hazard Analysis Techniques for System Safety*
- Everdij and Blom [50] – *Safety Assessment Techniques Database*

- EUROCONTROL [51] – *Review of Techniques to Support the EATMP Safety Assessment Methodology*
- FAA [17] – *Air Traffic Organization Safety Management System Manual* (version 2.1)
- FAA [16] – *System Safety Handbook*
- FAA/EUROCONTROL [52] – *ATM Safety Techniques and Toolbox*
- Kanemoto [53] – *ATM System Safety Methodology*
- Kritzinger [54] – *Aircraft System Safety: Military and Civil Aeronautical Applications*
- NASA [55] – *Dryden Handbook Code S System Safety Handbook*
- Netjasov and Janic [56] – *A Review of Research on Risk and Safety Modelling in Civil Aviation*
- Qureshi [57] – *A Review of Accident Modeling Approaches for Complex Critical Socio-Technical Systems*
- SAE [58] – *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*
- Stephans [59] – *Safety Systems for the 21st Century*
- Stolzer, Halford, and Goglia [60] – *Safety Management Systems in Aviation*
- System Safety Society [61] – *System Safety Analysis Handbook*

Of the documents mentioned above, EUROCONTROL [51], Everdij and Blom [50], FAA/EUROCONTROL [52], Qureshi [57], and Netjasov and Janic [56] describe and review both traditional and new techniques. Notably, EUROCONTROL and Everdij and Blom [50] reviewed more than 500 safety assessment techniques (detailed descriptions and reviews of those techniques are available in those documents). Based on the more than 500 techniques reviewed by EUROCONTROL, FAA/EUROCONTROL [52] identified 27 techniques that are in use and are most relevant to ATM safety:

- Air-MIDAS
- Air Safety Database
- ASRS (Aviation Safety Reporting System)
- Bias and Uncertainty Assessment
- Bow-Tie Analysis
- CCA (Common Cause Analysis)
- Collision Risk Models
- ETA (Event Tree Analysis)
- External Events Analysis
- FAST (Future Aviation Safety Team) Method
- FMECA (Failure Modes Effects and Criticality Analysis)
- FTA (Fault Tree Analysis)
- Future Flight Central
- HAZOP (Hazard and Operability study)
- HEART (Human Error Assessment and Reduction Technique)
- HERA (Human Error in ATM)
- HTA (Hierarchical Task Analysis)
- HTRR (Hazard Tracking and Risk Resolution)
- Human Error Database
- Human Factors Case
- PDARS (Performance Data Analysis and Reporting System)
- SADT (Structured Analysis and Design Technique)
- SAFSIM (Safety in Simulation)

- SIMMOD Pro (Simulation Model Professional)
- TOPAZ (Traffic Organization and Perturbation AnalyZer) accident risk assessment methodology
- TRACER-Lite
- Use of Expert Judgment

These techniques are representative and relevant to our study in that 1) they are all currently in use, 2) some of them are traditional or classical techniques such as Bow-Tie Analysis and FMECA, for relatively simple systems, and some are newer techniques such as TOPAZ accident risk assessment methodology, for relatively complex systems involving not only technical and human factors, but also organizational and other factors, and 3) they collectively cover all the steps of the SRM (hazard identification, risk analysis and assessment, and risk treatment). Although those techniques are biased towards those used for ATM, they are still somewhat the most relevant techniques for the air transportation system (thus very relevant to NextGen) because 1) ATM is a major part of the system, b) ATM is complex and some of the 27 methods are quite sophisticated in modeling the complexity involved in ATM and the entire air transportation system, and c) the methods used for ATM partly overlap with methods used for other aspects of the safety processes such as aircraft certification. For example, FTA and ETA are used in both ATM safety assessment and aircraft certification process. It needs to be noted that some of the 27 techniques are embedded in some others in the same list. For example, FTA and ETA are two components of Bow-Tie Analysis, and Bias and Uncertainty Assessment is part of TOPAZ accident risk assessment methodology. Also, some of the techniques not specifically listed are embedded in some of the 27 listed techniques. For example, TOPAZ accident risk assessment methodology uses the following techniques as its integral parts: DCPN (Dynamically Colored Petri Nets), Generalized Reich collision risk model, HSMP (Hybrid-State Markov Processes), TOPAZ-based hazard brainstorm, Monte Carlo Simulations, Markov Chains, Multiple Agent based modeling, PDP (Piecewise Deterministic Markov Processes), and so on [52].

For newer methods, we also reviewed the following:

- STPA (STAMP-based Analysis or System Theoretic Process Analysis): Leveson [30] – *Engineering a Safer World: System Thinking Applied to Safety*
- STPA and SD (System Dynamics): Dulac [62] – *A Framework for Dynamic Safety and Risk Management Modeling in Complex Engineering Systems*
- SD: Dulac et al. [63] – *Using System Dynamics for Safety and Risk Management in Complex Engineering Systems*
- SD: Ulrey and Shakarian [64] – *System Dynamics Application in Air Traffic Management: A Case Study*
- FRAM (Functional Resonance Analysis Method): Hollnagel [65] – *FRAM - the Functional Resonance Analysis Method: Modeling Complex Socio-Technical Systems*
- FRAM: EUROCONTROL [66] – *A White Paper on Resilience Engineering for ATM*
- SOAM (Systemic Occurrence Analysis Methodology): EUROCONTROL [67] – *Guidelines on the Systemic Occurrence Analysis Methodology (SOAM)*
- SoS (System of Systems) Hazard Analysis Simulation: Alexander [68] – *Using Simulation for Systems of Systems Hazard Analysis*
- BBN (Bayesian Belief Network): Ale et al [69] – *Causal Model for Air Transport Safety Final Report*
- AcciMap: Svedung and Rasmussen [70] – *Graphic representation of accident scenarios: Mapping system structure and the causation of accidents*

The following documents were reviewed for the methods used specifically for assessing NextGen safety (however, these methods and the traditional and newer methods mentioned above are not mutually exclusive):

- Fleming, Spencer, Leveson, and Wilkinson [71] – *Safety Assurance in NextGen*
- Consiglio, Hoadley, Wing, Baxley, and Allen [72] – *Impact of Pilot Delay and Non-Responsiveness on the Safety Performance of Airborne Separation*
- JPDO [73] – *Capability Safety Assessment of Delegated Interval Management*
- Morello and Ricks [74] – *Aviation Safety Issues Database*
- Zelkin and Henriksen [75] – *L-Band Digital Aeronautical Communications System Engineering – Initial Safety and Security Risk Assessment and Mitigation*
- Zelkin and Henriksen [76] – *C-Band Airport Surface Communications System Engineering – Initial High-Level Safety Risk Assessment and Mitigation*
- Rogers, Waldron, and Stroiney [77] – *Parametric Modeling of the Safety Effects of NextGen Terminal Maneuvering Area Conflict Scenarios*
- Ancel, Gheorghe, and Jones [78] – *NextGen Future Safety Assessment Game*
- Holmes, Sawhill, Herriot, and Seehart [79] – *Development of Complexity Science and Technology Tools for NextGen Airspace Research and Applications*
- Andrews, Welch, and Erzberger [80] – *Safety Analysis for Advanced Separation Concepts*
- Shortle, Sherry, Yousefi, and Xie [81] – *Safety and Sensitivity Analysis of the Advanced Airspace Concept for NextGen*
- Xu, Brown, Holford, Mast, Singleton, and Wilson [35] – *Socio-Technical Framework of Hazard Identification in Trajectory-based Operations*

Importantly, FAA's Integrated Safety Assessment Model (ISAM) for NextGen [82] is under the FAA's System Safety Assessment (SSA) project, which is part of the FAA's System Safety Management Transformation (SSMT) program. A key function or objective of ISAM is to identify potential negative and positive effects of NextGen OIs on safety.

> At its core, ISAM is a risk model that unifies sections from the EUROCONTROL Integrated Risk Picture (IRP) model…and from the Causal Model of Air Transport Safety (CATS)…The resulting hybrid model emphasizes the complementary contributions of both ATM and NAS users (flight crew and aircraft equipment) to safety events in the NAS…ISAM provides a comprehensive risk picture for air transport safety. [82, p. 3].

The IRP model was developed by EUROCONTROL [83] and the development of CATS was led by the National Aerospace Laboratory (NLR) in Netherlands [69]. Among others, ISAM includes Fault Tree Analysis (FTA) and Event Sequence Diagrams (ESDs) as its main techniques.

The System Safety Society has a list of risk assessment software, including program name, source, system, cost, and description for each of the programs [61, pp. B-1 – B-30]. Information on some software can also be found in a book titled, Aircraft System Safety: Military and Civil Aeronautical Applications [54] and at http://www.aircraftsystemsafety.com/default.asp.

4.4.2. Existing Safety Processes

Our review of the existing safety processes was largely based on the SRM process described in the FAA ATO (Air Traffic Organization) Safety Management Manual [17], the various safety processes summarized in Weibel and Hansman [84], and some of FAA's ongoing

process improvement and streamlining efforts outlined in its AVS Work Plan for NextGen 2012 [9]. Our review was also based on our experience of participation in safety assessments in industry standards development bodies such as RTCA and EUROCAE.

Numerous guidelines exist for how to conduct SRM:

- FAA ATO Safety Management System Manual [17]
- FAA System Safety Handbook [16]
- FAA Safety Risk Management Guidance For System Acquisitions (SRMGSA) [85]
- RTCA guidelines [e.g., 86]
- SAE guidelines [58]
- Mil-STD-882 [87]

See Figure 4 for the SRM steps or phases outlined in FAA ATO Safety Management System Manual [17].

One of our major findings, based on our experience of participation in safety assessments in industry standards development bodies, is that SRM is performed separately for different air transportation system components such as aircraft, operators, and air traffic management. This is confirmed by other studies [73], [84]. Sometimes the localized approach is also the case even within a component. That is, SRM is performed for individual elements of a component. For example, the development of requirements for systems supporting Flight Deck Interval Management – Spacing operations is considering the system that provides the guidance (speed change and maneuvers) and that will provide clearances for the most complex operations (CPDLC) separately, in two different committees. The Automatic Dependent Surveillance-Broadcast (ADS-B) application and FIM-S system are dealt with by RTCA SC-186/EUROCAE WG-51 joint committee, and the data communications side is being dealt with by RTCA SC-214/EUROCAE WG-78 joint committee. In addition, the work on aircraft capabilities is separate from that being performed to define required functionality in air traffic services (ATS) ground automation systems. These activities are conducted in parallel with very little coordination amongst them.

Similarly, different (and separate) safety approval or certification processes are used for different air transportation system components as described in Weibel and Hansman [84]:

- Aircraft and airborne equipment
- Airmen and air traffic controllers
- Operators
- Airspace procedure
- Separation standards and surveillance system performance
- Ground-based equipment and programs
- Software and complex electronic hardware
- Other safety control processes such as monitoring of current operations, and rulemaking

Figure 10 illustrates (albeit in a simplified version of the reality) the separate processes for aircraft certification, operator certification, and ATM approvals. For FAA's various certification and approval organizations, along with their roles and responsibilities, see FAA's AVS Work Plan for NextGen 2012 [9].

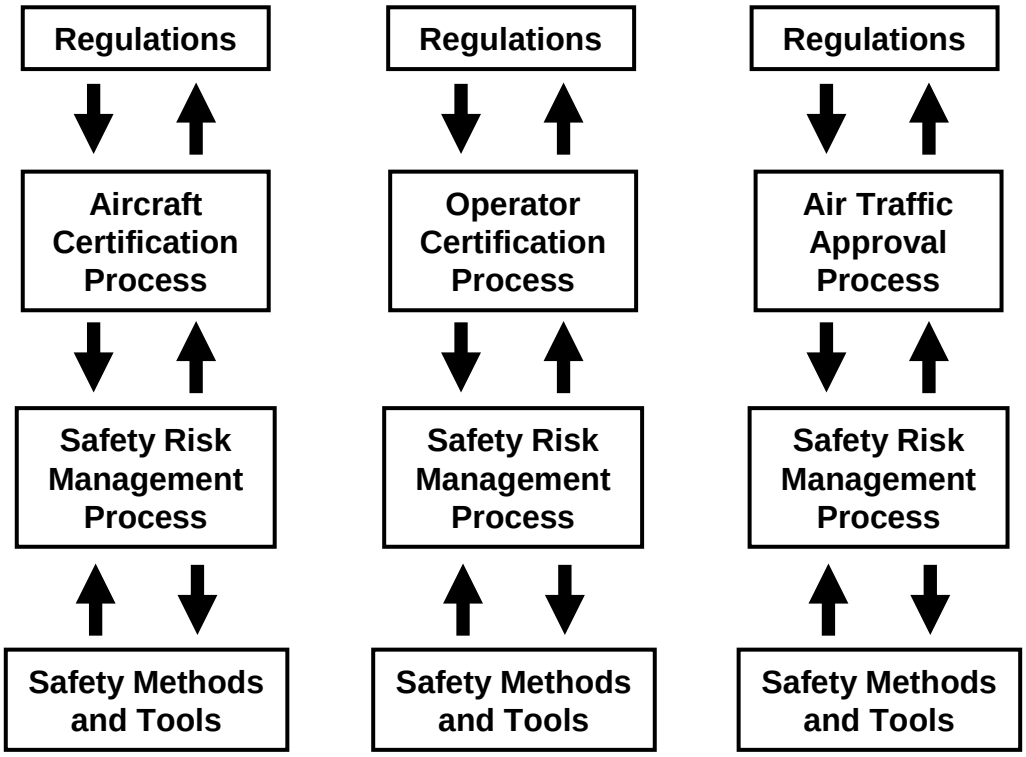


Figure 10. Separate Processes for Aircraft Certification, Operator Certification, and ATM Approvals

Faced with the challenges in NextGen, the FAA has been improving its various safety-related processes. According to FAA's AVS Work Plan for NextGen 2012 [9], AVS is streamlining certification processes for NextGen technologies in aircraft, including initiatives for improving the procedures and methodology of certification. It is also streamlining operational approval processes, including approval practices and procedures. Integration and coordination among the various AVS individuals and teams are also taking place involving the AVS Management Team (AVSMT), Service Management Leads for Aircraft Certification Service (AIR), Flight Standards Service (AFS), and Air Traffic Safety Oversight Service (AOV), and AVS NextGen Working Group. AIR, AFS, and AOV were primarily established for aircraft certification, operator certification, and air traffic approval, respectively. There is also coordination among AFS, AIR, and AOV in the field, as well as with the FAA headquarters offices (see Figure 11, [9, p. 34].

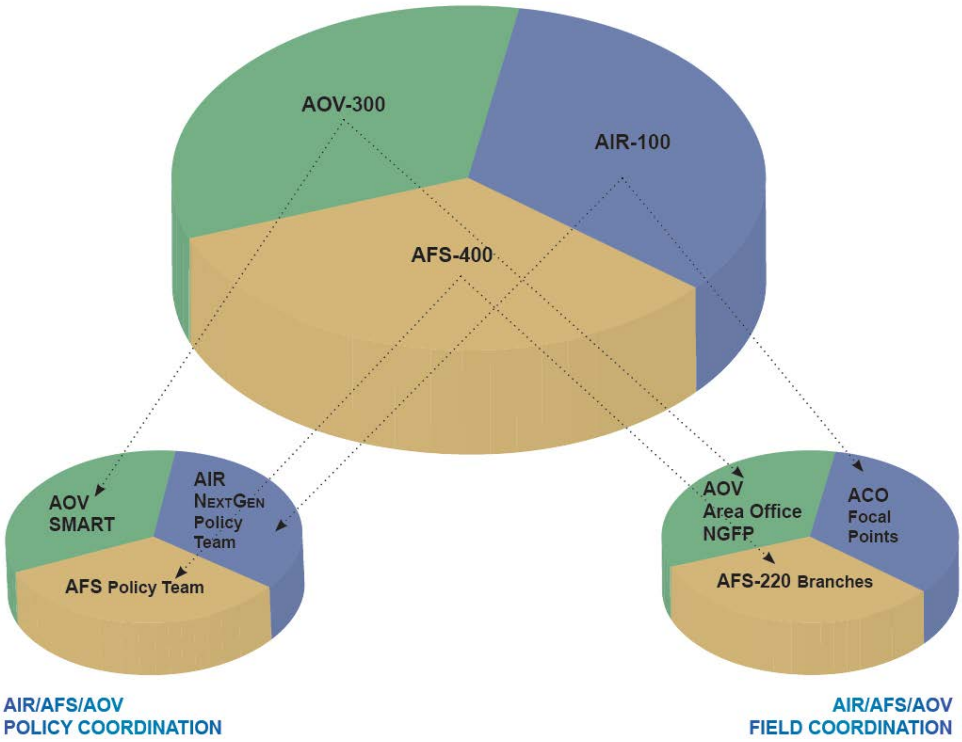


Figure 11. Coordination among FAA Headquarters and Other AVS Offices
Key: AFS = Flight Standards Service; AIR = Aircraft Certification Service; AOV = Air Traffic Safety Oversight Service; ACO = Aircraft Certification Office

4.4.3. Existing Safety Regulations

The documents we reviewed for the existing safety regulations are basically the same as those for the existing safety processes. Similar to the current safety processes, there are different (and separate) safety regulations for different air transportation system components in this country as summarized in Weibel and Hansman [84] (also see Figure 10):

- Aircraft airworthiness certification – Airworthiness standards are in FAR 23, 25, 27, 29, 31, 33, and 35.
- Certification of subcomponents of aircraft – There are certification processes including Supplemental Type Certificates (STC), Technical Standard Orders (TSO), and Parts Manufacturing Approval (PMA), which need to follow certain standards in FAA orders or advisory circulars.
- Certification of airmen and credentialing of air traffic controllers – Requirements must be met regarding training, medical examination, performance, and so on.
- Operator certificates and operational approval – FAR Part 91 (General Operating and Flight Rules) and FAR Part 121 (Operating Requirements: Domestic, Flag, and Supplemental Operation) must be followed, along with other certification requirements.
- Airspace procedure design and approval – The regulatory agency is FAA's Flight Standards Service (with the internal FAA designation of AFS), which establishes various rules such as visual flight rules and instrument flight rules, as well as designs and certifies various flight procedures, among others.

- Separation standards and surveillance system performance – ICAO guidance and FAA standards must be followed.
- Ground-based equipment and programs (i.e., air navigation facilities) – The FAA uses configuration management processes for tracking and coordinating changes to the NAS, and safety assessment is part of that.
- Software and complex electronic hardware – RTCA DO-178B [88] for airborne software certification, RTCA DO-278 [89] for non-airborne software in CNS/ATM systems, and RTCA DO-254 [86] for complex electronic hardware are the consensus standards. Although RTCA DO-178C has been published [90], the FAA has not yet referenced the document in materials that can be used in certification (e.g., Advisory Circulars). It is expected that the recognition of the use of RTCA DO-178C will happen eventually.

Again, according to FAA's AVS Work Plan for NextGen 2012 [9], the FAA and other organizations such as RTCA/EUROCAE are in the process of updating or developing standards and policies relevant to NextGen safety, including those for PBN/RNP, ADS-B, Data Communications, Low-Visibility Operations, Avionics Safety Enhancements, and Engine and Fuel Technologies.

4.5. Sufficiency of Existing Safety Methods, Tools, Processes, and Regulations

As our hazard analysis in the previous section shows, the safety situation in OI-0349 is rather challenging, where there are multiple components (aircraft, ground-based facilities, and ATC procedures), multiple factors (human, technical, organizational, and other factors), as well as dynamic complexity and interactions among the components and factors. An important question is whether the existing safety methods, tools, processes, and regulations are sufficient to ensure that the current level of safety is not compromised through the deployment of that OI. The following subsections describe our assessment regarding safety methods and tools, safety processes, and safety regulations, respectively.

4.5.1. Sufficiency of Existing Safety Methods and Tools

A set of criteria were developed based on the SRM steps described in FAA [17] and our Socio-Technical Framework of Hazard Identification [35]. Various safety methods and tools can be evaluated against the criteria below:

- Can a method or a tool cover multiple components (e.g., aircraft, ground-based facilities, and ATC procedures)?
- Can a method or a tool cover multiple factors (human, technical, organizational, and other factors)?
- Can a method or a tool capture dynamic interactions and complexity?
- Can a method or a tool facilitate systematic risk analysis and assessment?
- Can a method or a tool facilitate systematic risk treatment?

Table 2 shows the results of our sufficiency assessment of the various methods that we consider as most representative and most relevant to NextGen [52]. For illustration, below we provide a description of how we reached the ratings for two methods mentioned in this table: FTA (a traditional method) and TOPAZ accident risk assessment methodology (a newer method).

Table 2. Sufficiency of Most Representative Traditional and Newer Methods Safety Methods

Method	Cover multiple components (e.g., aircraft, ground facilities, and ATC procedures)?	Cover multiple factors (human, technical, organizational, and other factors)?	Capture dynamic interactions and complexity?	Facilitate systematic risk analysis and assessment?	Facilitate systematic risk treatment?
Air-MIDAS	Partly	Partly	Partly	Partly	Partly
Air Safety Database	Yes	Yes	No	Partly	Partly
ASRS (Aviation Safety Reporting System)	Yes	Yes	No	Partly	Partly
Bias & Uncertainty Assessment	Partly	Partly	No	Partly	Partly
Bow-Tie Analysis	Partly	Partly	No	Partly	Partly
CCA (Common Cause Analysis)	Partly	Partly	No	Partly	Partly
Collision Risk Models (Reich Model)	Partly	Partly	No	Partly	Partly
ETA (Event Tree Analysis)	Partly	Partly	No	Partly	Partly
External Events Analysis	Partly	Partly	No	Partly	Partly

Method	Cover multiple components (e.g., aircraft, ground facilities, and ATC procedures)?	Cover multiple factors (human, technical, organizational, and other factors)?	Capture dynamic interactions and complexity?	Facilitate systematic risk analysis and assessment?	Facilitate systematic risk treatment?
FAST (Future Aviation Safety Team) Method	Yes	Partly	No	Partly	Partly
FMECA (Failure Modes Effects and Criticality Analysis)	Partly	Partly	No	Partly	Partly
FTA (Fault Tree Analysis)	Partly	Partly	No	Partly	Partly
Future Flight Central	Partly	Partly	Partly	Partly	Partly
HAZOP (Hazard and Operability study)	Yes	Yes	No	Partly	Partly
HEART (Human Error Assessment and Reduction Technique)	Partly	Partly	No	Partly	Partly
HERA (Human Error in ATM)	Partly	Partly	No	Partly	Partly
HTA (Hierarchical Task Analysis)	Partly	Partly	No	No	No

Method	Cover multiple components (e.g., aircraft, ground facilities, and ATC procedures)?	Cover multiple factors (human, technical, organizational, and other factors)?	Capture dynamic interactions and complexity?	Facilitate systematic risk analysis and assessment?	Facilitate systematic risk treatment?
HTRR (Hazard Tracking and Risk Resolution)	Partly	Partly	No	Partly	Partly
Human Error Database	Partly	Partly	No	Partly	Partly
Human Factors Case	Partly	Partly	No	Partly	Partly
PDARS (Performance Data Analysis and Reporting System)	Partly	Partly	No	Partly	Partly
SADT (Structured Analysis and Design Technique)	Partly	Partly	No	Partly	Partly
SAFSIM (Safety in Simulation)	Partly	Partly	Partly	Partly	Partly
SIMMOD Pro	Yes	Yes	Partly	Partly	Partly
TOPAZ accident risk assessment methodology	Yes	Yes	Yes	Needs validation	Needs validation
TRACER-Lite	Partly	Partly	No	Partly	Partly

Method	Cover multiple components (e.g., aircraft, ground facilities, and ATC procedures)?	Cover multiple factors (human, technical, organizational, and other factors)?	Capture dynamic interactions and complexity?	Facilitate systematic risk analysis and assessment?	Facilitate systematic risk treatment?
Use of Expert Judgment	Partly	Partly	No	Partly	Partly

FTA is one of the most commonly used safety assessment methods. It is used for the analysis of hardware failures and to a certain extent of software problems in relatively simple systems. It is quite weak when it comes to analysis of human factors issues mainly because it is extremely difficult to assign probabilities to human errors. Its applicability to organizational factors and extra-organizational factors are also very limited. Therefore, it received "partly" for the "Cover multiple factors" criterion. Similarly, FTA is also limited when there are multiple components in a system, hence "Partly" for the "Cover multiple components" criterion. The tree structure of FTA does a fairly good job for relatively simple situations. For complex situations involved in the NextGen elements such as OI-0349, it would do a poor job because the complexity, especially the dynamic complexity, cannot be described by a fixed structure such as a tree [91]. This is the rationale for assigning "No" for the "Capture dynamic interactions and complexity" criterion. Based on those ratings, FTA also received "Partly" for the last two criteria: "Facilitate systematic risk analysis and assessment" and "Facilitate systematic risk treatment" Note: Some of the advanced versions of FTA such as dynamic fault tree analysis do a better job in modeling complexity [92].

TOPAZ accident risk assessment methodology, which was developed by researchers in NLR, is one of the most sophisticated modeling techniques. Using a set of tools, it is rather robust in identifying hazards from technical factors, human factors, procedures, and organizational factors. It is also comprehensive in that it can be used to model multiple components in a system. That is the reason why it received "Yes" for the first two criteria: "Cover multiple components" and "Cover multiple factors." This technique also does well in modeling the complex interactions among the multiple components and factors. The quantitative part of TOPAZ, known as multi-agent dynamic risk modeling (MA-DRM), has shown encouraging results when it was used to assess hazards and risks in complex situations (see [93] for a comparison between MA-DRM and ETA used in safety assessment of a runway incursion scenario). Meanwhile, new TOPAZ or MA-DRM methods and tools are being developed to further improve the modeling of complex interactions [93]. More recently, MA-DRM is being applied to some SESAR operations [94]. Based on our knowledge of this method, we assigned "Yes" for the "Capture dynamic interactions and complexity" criterion. Whether it can facilitate systematic risk analysis, assessment, and risk treatment to meet the target level of safety for SESAR operations, and similarly for NextGen operations, is a question. That is the reason for "Needs validation" regarding the last two criteria.

Table 3 shows the sufficiency assessment results of some other newer methods, in addition to those included in Table 2. As with the description of the rating process for FTA and TOPAZ

accident risk assessment methodology shown in Table 2, we provide a description of the rating process for two methods shown in this table: STPA and SOAM.

Table 3. Sufficiency of Other Newer Safety Methods

Method	Cover multiple components (e.g., aircraft, ground facilities, and ATC procedures)?	Cover multiple factors (human, technical, organizational, and other factors)?	Capture dynamic interactions and complexity?	Facilitate systematic risk analysis and assessment?	Facilitate systematic risk treatment?
STPA (STAMP-based Analysis)	Yes	Yes	Partly	Partly	Partly
SD (System Dynamics)	Yes	Yes	Yes	Partly	Partly
FRAM (Functional Resonance Analysis Method)	Yes	Yes	Partly	Partly	Partly
SOAM (Systemic Occurrence Analysis Methodology)	Yes	Yes	No	Partly	Partly
SoS (System of Systems) Hazard Analysis Simulation	Yes	Yes	Partly	Partly	Partly
Bayesian Belief Networks	Yes	Yes	No	Partly	Partly
AcciMap	Yes	Yes	No	Partly	Partly

STPA is a method developed by Professor Nancy Leveson at MIT. Based on STAMP (Systems Theoretic Accident Model and Processes), it takes a control theoretical view of system

safety and has many advantages compared to many traditional methods. It can be used to identify hazards arising from technical, human, and organizational factors and beyond, some of which cannot be identified using the traditional methods. It is also powerful when considering multiple components of a system. That is the reason why we assigned “Yes” to it for the “Cover multiple components” and “Cover multiple factors” criteria. It is robust in identifying many interactions among the multitude of factors and components, and to a certain extent, it can also support the identification of dynamic parts of system complexity. That is the basis for rating it as “Partly” for the last three criteria: “Capture dynamic interactions and complexity,” “Facilitate systematic risk analysis and assessment,” and “Facilitate systematic risk treatment.” It needs to be pointed out that the combination of STPA and SD seems to be a good approach because SD can augment STPA for capturing dynamic complexity as is shown in Dulac [62].

SOAM is a method developed by EUROCONTROL and is based on both the SHEL (Software, Hardware, Environment, and Liveware) model [20] and the Swiss cheese model [21]. The SHEL model is used for collecting safety-critical data taking into account factors from software, hardware, liveware or human, environment, and organization. The collected data are then used for guiding the identification of hazards in a Swiss cheese model-like framework with the following elements: human involvement, contextual conditions, organizational factors, and other system factors. It is also potentially useful for covering multiple components of a system. Thus, SOAM receives “Yes” for the “Cover multiple components” and “Cover multiple factors” criteria. However, the interactions among factors are not emphasized. Furthermore, it is basically a static approach, with no capability to capture the dynamic complexity associated with safety issues. This is the basis for assigning “No” for the “Capture dynamic interactions and complexity” criteria. As a result, although it is a useful method in some aspects, it “Partly” contributes to risk analysis, assessment, and treatment.

Table 4 shows the sufficiency assessment results of some of the methods and tools that have been used to assess NextGen safety. Below we describe the rating process for two methods whose results are shown in this table: Xu et al. [35] and Borener et al. [82].

Table 4. Sufficiency of Safety Methods Used for NextGen Operations

Method	Cover multiple components (e.g., aircraft, ground facilities, and ATC procedures)?	Cover multiple factors (human, technical, organizational, and other factors)?	Capture dynamic interactions and complexity?	Facilitate systematic risk analysis and assessment?	Facilitate systematic risk treatment?
Fleming, Spencer, Leveson, and Wilkinson [71]	Yes	Yes	Partly	Partly	Partly

Method	Cover multiple components (e.g., aircraft, ground facilities, and ATC procedures)?	Cover multiple factors (human, technical, organizational, and other factors)?	Capture dynamic interactions and complexity?	Facilitate systematic risk analysis and assessment?	Facilitate systematic risk treatment?
Consiglio, Hoadley, Wing, Baxley, and Allen [72]	Partly	Partly	No	Partly	Partly
JPDO [73]	Yes	Partly	No	Partly	Partly
Morello and Ricks [74]	Yes	Yes	No	Partly	Partly
Zelkin and Henriksen [75]	Partly	Partly	No	Partly	Partly
Zelkin and Henriksen [76]	Partly	Partly	No	Partly	Partly
Rogers, Waldron, and Stroiney [77]	Partly	Partly	No	Partly	Partly
Ancel, Gheorghe, and Jones [78]	Yes	Yes	Partly	Partly	Partly
Holmes, Sawhill, Herriot, and Seehart [79]	Partly	Partly	Partly	Partly	Partly

Method	Cover multiple components (e.g., aircraft, ground facilities, and ATC procedures)?	Cover multiple factors (human, technical, organizational, and other factors)?	Capture dynamic interactions and complexity?	Facilitate systematic risk analysis and assessment?	Facilitate systematic risk treatment?
Andrews, Welch, and Erzberger [80]	Partly	Partly	No	Partly	Partly
Shortle et al. [81]	Partly	Partly	Partly	Partly	Partly
Xu, Brown, Holford, Mast, Singleton, and Wilson [35]	Yes	Yes	No	Partly	Partly
Borener, Trajkov, & Balakrishna [82]	Yes	Yes	No	Partly	Partly

Our Socio-Technical Framework of Hazard Identification [35] is a high-level hazard identification and analysis method. It was used for a preliminary hazard analysis applied to Trajectory-Based Operations (TBO), one of the key NextGen pillars [35]. This method is quite comprehensive in that it can guide the identification of hazards from human, technical, environmental, organizational, and other factors that are involved in multiple components including aircraft, ground-based facilities, ATC procedures, and so on. This is the basis for receiving "Yes" for the "Cover multiple components" and "Cover multiple factors" criteria. It can also guide high-level identification of interactions among those components and factors. However, it is rather weak when it comes to revealing dynamic interactions. Therefore, it receives "No" for "Capture dynamic interactions and complexity" and it can partly contribute to the systematic risk analysis, assessment, and treatment; hence, "Partly" for the last two criteria.

The FAA's Integrated Safety Assessment Model (ISAM) for NextGen as summarized in Borener et al. [82] is a comprehensive approach to assessing primarily the safety impacts of NextGen OIs. It encompasses multiple personnel and system components including both ATM and other NAS users such as flight crew and aircraft equipment, and it may include Airlines Operation Centers (AOC) in a future version. Therefore, it receives "Yes" regarding the first two criteria. As far as we know, FTA and Event Sequence Diagrams (ESDs) are its main assessment methods. As we illustrated for FTA, which is rated in Table 2, the tree structure of the two methods is limited for modeling dynamic complexity, leading us to assigning "No " for

the “Capture the dynamic interactions and complexity” criteria and as a result, “Partly” for the last two criteria. It is recognized that within ISAM, analysis methods and tools are being developed or improved, including near real-time analysis tools that can be used to identify risks in new operations [82]. This is thus an evolving method and its modeling capabilities are expected to be improving.

Based on the above results, it can be concluded the traditional methods such as FTA, ETA, and FMECA are insufficient because they are far from being able to capture the dynamic complexity of NextGen, and cover multiple components and factors therein. Some of the newer ones such as STPA, SD, FRAM, TOPAZ accident risk assessment methodology, and BBN are better than the traditional methods in that respect. Whether a technique is sufficient for NextGen safety has also to do with NextGen’s required level of safety; the higher the required level of safety, the more sophisticated a technique needs to be. On one hand, NextGen is believed to be more complex than the current system; on the other hand, it needs to be safer than the current system. Therefore, the sufficiency of some of the newer techniques for NextGen safety is a question as well as a concern, and their adequacy requires proof or validation relative to the required level of safety. The ongoing methods also need proof or validation for NextGen safety.

Regarding the sufficiency of tools (various computer programs or software), they are generally only as good as the methods they are based on. Therefore, the tools are mostly not sufficient for NextGen safety or need validation.

4.5.2. Sufficiency of Existing Safety Processes

Overall, the existing processes are not sufficient because SRM and approval and certification processes are performed for individual components (e.g., aircraft, ground-based facilities, and air traffic control procedures), but not for the whole system when they function together [73], [84]. It is thus doubtful that the complex interactions among the components are adequately identified and addressed. Some of them are not even sufficient for individual components:

- SRM processes need to be improved [95].
- There is room for improvement in the certification and approval processes [47], [48].

Our assessment is consistent with JPDO [73], which states the following:

> To ensure NextGen safety, it is necessary to assess the system as a whole, which means it must be designed as a whole. Often, systems are designed and assessed as individual pieces with the expectation that if the subsystems are safe, the system will be safe. A piece-wise approach is seen throughout the aviation system. Aircraft, airports, airspace, air traffic management, and flight crews are individually certified as safe, and then expected to remain safe when functioning together. As NextGen introduces an ever-widening range of variables, it is even more critical that NextGen be designed and implemented as an integrated ‘safety of the whole’ system. [73, pp. 24-25].

Although the FAA is streamlining its certification and approval processes, and integration and coordination within the agency are improving, it needs to be seen whether those efforts are sufficient to address NextGen safety as an entirety, rather than in a stovepipe fashion.

4.5.3. Sufficiency of Existing Safety Regulations

There are inherent shortcomings in regulations. Regulations cannot cover everything; they tend to compartmentalize things; they are slow to keep up with technology changes; and they can be too prescriptive [54]. These weaknesses will manifest themselves more when faced with the NextGen complexity. Further, the regulations do not appear to be sufficient because different standards and requirements are imposed for the safety of individual components, but not for the safety of the whole system. Similar to the FAA's efforts to streamline its certification and approval processes, the FAA needs to show that its work to update and develop safety-related standards is sufficient to meet NextGen safety requirements. In fact, the FAA AVS acknowledges the need to evaluate the relevant operational regulations, to identify needed changes to regulations, and to develop new regulations [9].

4.6. Costs of Existing Safety Methods, Tools, Processes, and Regulations

Another important question is whether the existing methods, tools, processes, and regulations might incur intolerably high costs for assessing and ensuring NextGen safety. In this study, cost assessment was performed qualitatively rather than quantitatively. Given that the current approach is mostly insufficient for assuring NextGen safety, we assessed the costs first in terms of those associated with an inadequate approach (methods, tools processes, and regulations). Cost assessment can also be conducted in terms of those associated with developing and implementing an adequate approach.

4.6.1. Costs of Inadequate Approach

The existing methods, tools, processes, and regulations rely on the known performance of existing systems, and safety assessments are conducted for single changes or minor changes. That is not the way NextGen elements are likely to be introduced. Rather, many of them will be introduced at the same time or within short intervals. Therefore, this existing approach would take an intolerably long time (because it is only appropriate for incremental changes introduced in a serial fashion), and would need a lot of resources to assess the safety of NextGen elements and yet still not likely to achieve the required NextGen level of safety because of the NextGen complexity.

Inadequate safety methods, tools, processes, and regulations can lead to incorrect conclusions being drawn and inappropriate requirements set. As a result, systems can be developed that do not provide the level of performance required to keep system safety at or above the preceding level. In many cases, the conservative nature of the safety processes means that the level of safety will be preserved, but this will not always be the case. Inadequacies may be discovered during airworthiness certification or during operational approval, or even after the new operational function is in revenue service. In such cases, the regulator imposes additional or different requirements, and these changes are rolled back into published requirements that will govern the design of systems for forward fit. Operators may be required to update or replace systems already in service, sometimes at significant cost. During transition from old to new systems, whether through retrofit or through addition to or replacement of aircraft in their fleets, operators must maintain spares of both standards to ensure that failures can be corrected with the appropriate parts. This increases spares holdings at additional cost to the operator. Even software changes in the same hardware can result in a part number change that creates the same lack of commonality among those aircraft on which the service bulletin has been satisfied and those on which it has not, and a similar requirement for additional spares and close management of maintenance and repair functions. An example of such a series of events follows.

During the 1990s, Europe determined that transponder capabilities (specifically the availability of only 4096 Mode A codes) were inadequate to ensure that each aircraft operating during a day could be issued with a unique Mode A code, and developed a mandate for what was known as 'Elementary Surveillance' (ELS). ELS would add to the capabilities of the aircraft transponder by transmitting on Mode S the individual aircraft's 24-bit ICAO address to be used as a unique form of identification. At the same time, requirements for 'Enhanced Surveillance' (EHS) were written for later implementation. However, some European states determined that there would be benefit in their receiving the additional data transmitted by EHS, and replaced the ELS mandate with one for EHS. The avionics manufacturers saw an opportunity to develop a transponder that satisfied current Mode A, C and S requirements plus both ELS and EHS. Also, because the FAA and EUROCONTROL had agreed that the transmission medium for ADS-B should be Mode S (at least for aircraft likely to operate internationally), it would be a good opportunity to incorporate the ADS-B function into the new transponder.

Unfortunately, stand-alone requirements for ADS-B Out were still in development at that time, but a higher-level standard was available, and it was to this that the included ADS-B Out function was designed. This became the 'DO-260-like' version (Version 0) of ADS-B Out. As operators began to equip with transponders that would satisfy ELS and EHS mandates, many chose to satisfy the service bulletin that would activate the ADS-B Out function; however, the ADS-B functionality was not certified for anything but "non-interference," and a Flight Manual addition proscribed its operational use. By the time Boeing began to install these transponders (early 2004), the shortcomings of the ADS-B standard had been recognized and a new standard (DO-260A) had been published. However, since the ELS/EHS mandate was imminent, it was not possible to satisfy DO-260A requirements at that time.

Both Europe and the United States then set dates for mandates for ADS-B Out equipage, but the FAA recognized that the ATS ground system could not function well without the transponder Mode A code's being included in the ADS-B message, so a new standard, DO-260B was developed and published. It is to this standard that mandated equipage must be responsive in the United States, and in response to a desire for interoperability, also in Europe. However, ADS-B is, by its nature, a data gathering and transmitting function, and the United States and Europe have specified different data quality requirements in their mandates, illustrating a parallel issue with safety assessment methods (that different methods and/or different practitioners result in different answers to the same question). As a result, interoperability will not be achieved, and for aircraft operating in the United States, the vast majority of GPS receivers will have to be replaced to satisfy ADS-B data quality requirements, again at additional cost.

In the meantime, significant operational trials have been conducted in Europe utilizing the original Version 0 equipment as a surveillance data source for ground surveillance and separation assurance. The safety case used to show that Version 0 satisfied requirements was adopted by other countries, not on a trials basis, but for permanent operational use, and benefits are being derived from the Version 0 equipment in ATS procedures for which other states judge the system unsafe. The FAA's ground system will not send Version 0 data to controller screens, and the FAA has stated that only DO-260B data will be usable for separation services. However, an exception has been made for some operations in the FAA-controlled portion of the Gulf of Mexico, where DO-260A equipment is providing surveillance data that is used for separation services.

This is a good illustration of the issues that can arise when new technologies and new procedures associated with both new and current technologies are introduced. There will be

little understanding of the new procedures and the technical functions needed to support them in the aviation community as a whole. Requirements are developed by groups of technical and operational experts who are extending their horizons to understand what is expected. Many participants are there on a voluntary basis representing manufacturers, operators, and professional organizations, each with an agenda to satisfy; others are representatives of the ATS provider and regulator with goals that relate to meeting deadlines and completing projects. In development of requirements for operational applications supported by ADS-B data on the flight deck, despite the fact that ATS ground system functionality will be required to enable a beneficial operation, the standards groups have not been permitted to levy requirements against the ground system. Resulting standards can only make assumptions about future ground system functionality, assumptions that have no guarantee of being met. If they are not met, how valid will the requirements levied against the airborne systems be? If these kinds of past lessons are not learned, the same or similar issues may emerge during the transition to, and implementation of, NextGen.

Further, because different methods, tools, processes, and regulations exist for different components (e.g., aircraft, ground-based facilities, and ATC), resources may not be utilized in an optimized way, yet again likely without achieving the required NextGen level of safety. Costs of this approach also include those of not providing the required level of safety for NextGen including, at one extreme, a potentially intolerable number of accidents, but more likely limiting the benefits available through added operational conservatism and ultimately by requiring system upgrades to achieve the desired levels of safety and operational benefit.

4.6.2. Costs of Adequate Approach

The type of approach to NextGen safety, by use of systematic methodology and of integrated tools, processes, and regulations, is likely to demand high levels of expertise and technological support. These resources will be employed over a significant timeframe. That is, methods and tools must be validated to show that hazards resulting from dynamic complexity of the combination of NextGen elements under consideration can be reliably identified while taking into account multiple components and multiple factors, and the resultant risks can be adequately treated. Processes and regulations must also be developed or modified to be adequate given the dynamic complexity. The need to coordinate among the large number of air transportation system stakeholders will add to the time taken to develop acceptable methods and to work through the safety processes. The result of satisfying such needs is inevitably higher cost.

Despite the length of time that will have to be dedicated to an adequate safety approach, it is likely that the time taken to achieve an acceptable outcome in the form of an air transportation system that is safe and efficient in accommodating traffic demand will be shorter than that taken if an inadequate safety approach is used. In the latter case, the initial time may be relatively shorter, but the result may fall short of the targeted level of safety, resulting in constraints being placed on capacity or efficiency until safety levels can be raised by additional effort. While costly in the short term, the adequate approach can be expected to cost less overall than the inadequate approach. The adequate approach will result in an optimal combination of safety, efficiency, and capacity without need for changes in the form of avionics retrofit, procedure amendment, additional training, and ground system modification, all of which are costly. The tolerability of the cost of providing an adequate approach to safety assurance must be weighed against the benefits that might be derived in terms of efficiency and capacity and also against the potential costs of an inadequate approach.

5. Conclusions

We surveyed a large number of NextGen documents and databases, and identified NextGen elements in the form of Operational Improvements (OIs), Enablers, Research Activities, Development Activities, and associated Policy Issues from the JPDO's NextGen Integrated Work Plan (IWP), the FAA Enterprise Architecture (NAS EA), and the FAA NextGen Implementation Plan (NGIP).

Several features of NextGen may contribute to the overall challenging hazard situation, including higher traffic density, higher levels of automation, more tightly-coupled operations, more decentralized operations, and the introduction of multiple elements within a short time. For a representative NextGen OI, OI-0349 (Automation Support for Separation Management), we performed a high-level hazard analysis, which is a preliminary hazard analysis in the concept phase of a system's life cycle. More specifically, we used our Socio-Technical Framework of Hazard Identification to identify high-level hazards, illustrating how interactions among various factors may generate hazards. For a scenario of OI-0349 with high levels of both airborne and ground automation, we identified hazards in Flight Deck Interval Management – Spacing (FIM-S), highlighting the potential level of dynamic complexity not experienced in operations in the current system.

The safety of NextGen depends largely on the sufficiency of safety methods, tools, processes, and regulations. The existing methods and tools, especially those used in the United States, do not appear to be sufficient to identify the hazards in the NextGen elements and assess their risks given the high degree of dynamic complexity in the elements. Some (e.g., STPA, SD, FRAM, TOPAZ) may be better than others, but need proof. The processes and regulations in this country are also not sufficient because individual components are assessed and approved separately, but not as a whole system. Some of them are not sufficient even for the individual components. From the system and control-theoretical perspective [30], the insufficient methods, tools, processes, and regulations themselves may impose a significant hazard to NextGen safety.

Further, inadequate methods, tools, processes, and regulations might incur intolerably high costs in the long term, including costs of not meeting the required NextGen safety level. On the other hand, an adequate approach can also be costly because of the time and resources required for the development, validation, and implementation. However, its costs should be weighed against the costs of an inadequate approach.

6. Recommendations

Based on the above assessments, we would like to make several recommendations, which we beelive may lead to improvements. The first set of recommendations outlines what needs to be done with respect to safety methods, tools, processes, and regulations for NextGen safety:

- Identify or determine the desired or target level of safety in NextGen because it has implications for whether methods, tools, processes, and regulations are sufficient.
- Be innovative on new methods and tools including exploration of combining or integrating the existing ones (e.g., combining or integrating two or more of, FTA, User of Expert Judgment, STPA, SD, BBN, TOPAZ, and SIMMOD Pro). This is not only necessary for individual NextGen elements, but also important for interactions among OIs, and for the entire NextGen.

- Sort out the relationship among various safety techniques and tools and compare their relative effectiveness.
- Continue developing and modifying processes and regulations.
- Validate new or proposed methods, tools, processes, and regulations.
- Coordinate methods, tools, processes, and regulations so that they can work together to achieve NextGen's required level of safety.
- Further assess the costs of an inadequate safety approach and an adequate approach.

What are also needed are more systematic assessments of the safety methods, tools, processes, and regulations associated with SESAR. SESAR bears many similarities to NextGen and its safety challenges are similar to those of NextGen. Our preliminary assessment of SESAR suggests that the standard or old methods, tools, processes, and regulations in Europe are not sufficient for SESAR safety. Numerous efforts in Europe are addressing this inadequacy. The United States can adopt some of the European approaches and practices. For example, inspirations can be taken and lessons can be learned from dynamic risk modeling [92], which has been applied to the safety assessment for some current operations in Europe and is being applied to SESAR operations [96], [97]. In fact, there have been collaborations between the United States and Europe regarding NextGen and SESAR safety (e.g., [82]). Information exchanges regarding NextGen and SESAR are also important for interoperability between the two systems and have important global implications.

7. References

[1] Joint Planning and Development Office, *Concept of Operations for the Next Generation Air Transportation System (NextGen), Ver. 3.2,* Sept. 30, 2010. Available: http://jpe.jpdo.gov/ee/docs/conops/NextGen_ConOps_v3_2.pdf

[2] Joint Planning and Development Office, *NextGen Enterprise Architecture (EA),* 2012. Available: http://jpe.jpdo.gov/ee/request/home

[3] Joint Planning and Development Office, *Integrated Work Plan for the Next Generation Air Transportation System, 2012*. Available: http://jpe.jpdo.gov/ee/request/home

[4] Joint Planning and Development Office, *Targeted NextGen Capabilities for 2025,* Nov. 2011. Available: http://www.jpdo.gov/library/2011_Targeted_NextGen-Capabilities_for_2025_v3.25.pdf

[5] Joint Planning and Development Office, *Net-Centric Operations Concept of Operations, Ver. 1.0,* Jul. 7, 2010. Available: http://www.jpdo.gov/library/20100701_NCO_ConOps_v1.0.pdf

[6] Joint Planning and Development Office, *JPDO Trajectory-Based Operations (TBO) Study Team Report,* Dec. 4, 2011. Available: http://www.jpdo.gov/library/TBO%20Study%20Team%20Report.pdf

[7] Federal Aviation Administration, *National Airspace System Enterprise Architecture* (NAS EA Portal 7.9), 2012. Available: https://nasea.faa.gov/

[8] Federal Aviation Administration, *NextGen Implementation Plan*, Mar. 2012, Available: http://www.faa.gov/nextgen/implementation/media/NextGen_Implementation_Plan_2012.pdf

[9] Federal Aviation Administration, *AVS Work Plan for NextGen,* Mar. 2012. Available: http://www.faa.gov/nextgen/media/avs_nextgen_workplan_2012.pdf

[10] Federal Aviation Administration, *2009-2013 FAA Flight Plan,* [n.d.] Available: http://www.faa.gov/about/plans_reports/media/flight_plan_2009-2013.pdf

[11] Federal Aviation Administration, *National Aviation Research Plan (2011),* May 2011. Available: http://www.faa.gov/about/office_org/headquarters_offices/ang/offices/ac_td/research_planning/narp/media/pdf/NARP_2011.pdf

[12] Federal Aviation Administration, *National Airspace and Procedure Plan 2010,* Jan. 11, 2011. Available: http://www.faa.gov/nextgen/media/NAPPecopy.pdf

[13] Federal Aviation Administration, *FAA AVS Work Plan for Next Gen 2011,* Apr. 2, 2011. Available: http://www.faa.gov/nextgen/media/AVS%20Work%20Plan%20for%20NextGen%202011.pdf

[14] E. G. Waggoner, "The NextGen integrated work plan," JPDO Briefing, Apr. 28, 2010. Available: http://www.jpdo.gov/library/PartnerAgency/IWP_ED.pdf

[15] Joint Planning and Development Office, *Integrated Work Plan for the Next Generation Air Transportation System Executive Summary, Ver. FY13*, [n.d.]. Available: http://jpe.jpdo.gov/ee/docs/pdf/IWP_FY13_Executive_Summary.pdf

[16] *System Safety Handbook*, Washington, DC: Federal Aviation Administration, 2008. Available: http://www.faa.gov/library/manuals/aviation/risk_management/ss_handbook/

[17] Federal Aviation Administration, *Air Traffic Organization Safety Management System Manual* (version 2.1), May 27, 2008. Available: http://www.faa.gov/air_traffic/publications/media/ATOSMSManualVersion2-1_05-27-08_Final.pdf

[18] International Civil Aviation Organization, *Safety Management Manual (SMM),* 2nd ed. Montreal, Canada: ICAO, 2009. Available: http://www.icao.int/safety/ism/Guidance%20Materials/DOC_9859_FULL_EN.pdf

[19] F. Hawkins, *Human Factors in Flight.* Brookfield, VT: Gower Technical Press Ltd., 1987.

[20] E. Edwards, "Man and machine: Systems for safety," In *Proc. of British Airline Pilots Associations (BALPA) Tech. Symp.*, London, UK, 1972, pp. 21-36.

[21] J. Reason, *Human Error.* Cambridge, U.K.: Cambridge Univ. Press, 1990.

[22] The System of Systems Engineering Center of Excellence. (n.d.). *The System of Systems Engineering Center of Excellence.* Available: http://www.sosece.org/library/SoSECE%20Brochure%2010-13.pdf

[23] P. Brooker, "Air traffic safety: Continued evolution or a new paradigm?" *Aeronautical J.,* vol. 112, no. 1132, pp. 333-343, Jun. 2008.

[24] C. Perrow, *Normal Accidents: Living With High-Risk Technologies (with a new afterword and a postscript on the Y2K problem).* Princeton, NJ: Princeton Univ. Press, 1999.

[25] A. Pritchett, "NextGen aviation safety," in *Nat. Workshop for Research on High-Confidence Transportation Cyber-Physical Systems: Automotive, Aviation & Rail***,** Washington, DC, 2008. Available: http://www.ee.washington.edu/research/nsl/aar-cps/Pritchett_NSFCPS.pdf

[26] A. Pritchett, "The system safety perspective," in *Human Factors in Aviation,* 2nd ed., E. Salas and D. Maurino, Eds. Burlington, MA: Academic Press, 2010.

[27] J. Hansman, *Statement of R. John Hansman, Jr., T. Wilson Professor of Aeronautics & Astronautics and Engineering Systems, Director, MIT International Center for Air Transportation, Massachusetts Institute of Technology Before the U.S. House of Representatives, Subcommittee on Space and Aeronautics, House Committee on Science*, February 16, 2011. Available: http://science.house.gov/sites/republicans.science.house.gov/files/documents/021611_Hansman.pdf

[28] P. M. Senge, *The Fifth Discipline: The Art and Practice of the Learning Organization.* New York: Currency Doubleday, 2006.

[29] N. G. Leveson, "A new accident model for engineering safer systems," *Safety Sci., vol.* 42, no. 4, pp. 237-270, 2004.

[30] N. G. Leveson, *Engineering a Safer World: System Thinking Applied to Safety.* Cambridge, MA: MIT Press, 2011. Available: http://mitpress.mit.edu/books/engineering-safer-world

[31] U.S. House of Representatives Committee Hearing on Science and Technology, 110th Congress, 2nd session, *Hearing on the Next Generation Air Transportation System: Status and Issues*, Sept. 11, 2008. Available: http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg44270/html/CHRG-110hhrg44270.htm

[32] L. Werfelman, "Bad parts," *Aerospace World*, vol. 6, no. 3, pp. 13-15, Apr. 2011. Available: http://flightsafety.org/download_file.php?filepath=/asw/apr11/asw_apr11_p13-15.pdf

[33] R. Parasuraman *et al.,* "A model for types and levels of human interaction with automation," *IEEE Trans. Syst. Man Cybern. A., Syst Humans,* vol. 30, pp. 286-297, May 2000.

[34] Radio Technical Commission for Aeronautics, "NextGen mid-term implementation task force report," RTCA, Washington, DC, 2009.

[35] X. Xu, *et al.,* "Socio-technical framework of hazard identification in trajectory-based operations," in *Proc. 30th Digital Avionics Systems Conf.,* Seattle, WA, 2011.

[36] Joint Planning and Development Office, *NextGen Avionics Roadmap, Ver. 2.0*, Sept. 30, 2011. Available: http://www.jpdo.gov/library/20111005_ARM_complete_LowRes_v2.0.pdf

[37] Office of Internal Governance, "Enhanced oversight of staffing and training at FAA's critical facilities is needed to maintain continuity of operators," United States Dept. Transportation, Washington, DC, Rep. AV-2012-039, 2012. Available: http://www.oig.dot.gov/node/5708

[38] C. O. Miller, "System safety," in *Human Factors in Aviation,* 1st ed. E.L. Wiener and D. C. Nagel, Eds. New York: Academic Press, 1988, pp. 53-79.

[39] Joint Planning and Development Office, *Safety Management System Standard v1.4,* Jul. 30, 2008. Available: http://www.jpdo.gov/library/InformationPapers/JPDO_SMS_SPC_v1_4.pdf

[40] Joint Planning and Development Office, *ATM-Weather Integrated Plan, Ver. 0.8*, Apr. 22, 2009. Available: http://test.jpdo.gov/library/atm-weather_2/ATM-Weather_Integration_Plan_v0-8_without_attachments.pdf

[41] K. Allendoerfer *et al.*, "Human factors analysis of safety alerts in air traffic control," FAA, Atlantic City, NJ, DOT/FAA/TC-07/22, 2007. Available: http://hf.tc.faa.gov/technotes/dot_faa_tc_07_22.pdf

[42] E. Rovira and R. Parasuraman,"Transitioning to future air traffic management: Effects of imperfect conflict-probe automation on controller attention and performance," *Human Factors*, vol.52, no.3, pp.412-425, Jun. 2010. Available: http://archlab.gmu.edu/people/rparasur/Documents/RoviraParasuramanHF2010.pdf

[43] P. Kopardekar, *et al.,* "Feasibility of mixed equipage operations in the same airspace," in *Proc. 8th USA/Europe Air Traffic Management Research and Development Seminar,* CA, 2009, pp. 1-9. Available: http://www.atmseminar.org/seminarContent/seminar8/papers/p_089_DACM.pdf.

[44] Joint Planning and Development Office, *National Aviation Safety Strategic Plan, Ver. 1.0B,* Jun. 10, 2011. Available: http://www.jpdo.gov/library/20110610_NASSP_V1.0b.pdf

[45] Government Accountability Office, "Next Generation Air Transportation System: FAA faces challenges in responding to Task Force Recommendations," GAO, Washington, DC, Rep. GAO-10-188T, 2009. Available: http://www.gao.gov/assets/130/123636.pdf

[46] Government Accountability Office, "Aviation safety: FAA's safety oversight system is effective but could benefit from better evaluation of its programs' performance," GAO, Washington, DC, Rep. GAO-06-266T, 2005. Available: http://www.gao.gov/assets/90/82201.pdf

[47] Aircraft Certification Process Review and Reform Aviation Rulemaking Committee, *A Report from the Aircraft Certification Process Review and Reform Aviation Rulemaking Committee to the Federal Aviation Admin.: Recommendations on the Assessment of the Certification and Approval Process,* May 22, 2012. Available: http://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/ACPRR.ARC.RR.May.22.2012.pdf

[48] Government Accountability Office, “Aviation safety: Certification and approval processes are generally viewed as working well, but better evaluative information needed to improve efficiency,” GAO, Washington, DC, Rep. GAO-11-14, Oct. 2010. Available: http://www.gao.gov/assets/320/311045.pdf

[49] C. Ericson, *Hazard Analysis Techniques for System Safety.* Hoboken, NJ: Wiley, 2005.

[50] M. H. C. Everdij *et al. Safety Assessment Techniques Database* (version 0.9), Dec. 7, 2010. Available: http://www.nlr.nl/downloads/safety-methods-database.pdf

[51] EUROCONTROL, “Review of techniques to support the EATMP safety assessment methodology vol. 1,” EUROCONTROL, France, January 2004. Available: http://www.eurocontrol.int/eec/public/standard_page/DOC_Report_2004_001.html

[52] Federal Aviation Administration and EUROCONTROL, “ATM safety techniques and toolbox,” FAA and EUROCONTROL, Safety Action Plan-15, version 2.0, Oct. 2007. Available: http://www.eurocontrol.int/eec/gallery/content/public/document/eec/report/2007/023_Safety_techniques_and_toolbox.pdf

[53] M. M. Kanemoto, “ATM system safety methodology,” Boeing Co., Seattle, WA, Rep. D780-10069-1, 2002.

[54] D. Kritzinger, *Aircraft System Safety: Military and Civil Aeronautical Applications.* Cambridge, UK, Woodhead Publ. Ltd., 2006.

[55] *Dryden Handbook Code S System Safety Handbook*, NASA Dryden Flight Research Ctr., Edwards, CA, 1999. Available: http://www.hnd.usace.army.mil/safety/RefDocs/FASS/NASA%20Systems%20Safety.pdf

[56] F. Netjasov and M. Janic, “A review of research on risk and safety modelling in civil aviation,” *J. Air Transport Manage.,* vol. 14, no. 4, pp. 213-220, Jul. 2008.

[57] Z. H. Qureshi, “A review of accident modeling approaches for complex critical socio-technical systems,” DSTO Defence Sci. & Technology Organisation, C3I Div., Edinburgh, Australia, Rep. DSTO-TR-2094, 2008. Available: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA482543

[58] Society of Automotive Engineers, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment,* SAE ARP 4761, 1996.

[59] R. A. Stephans, *System Safety for the 21st Century: the Updated and Revised Edition of System Safety 2000.* Hoboken, NJ: Wiley & Sons, 2004.

[60] A. J. Stolzer *et al.*, *Safety Management Systems in Aviation.* Burlington, VT: Ashgate, 2008.

[61] *System Safety Analysis Handbook*, 2nd ed., Albuquerque, NM: System Safety Society New Mexico Chapter, 1997.

[62] N. Dulac, “A framework for dynamic safety and risk management modeling in complex engineering systems,” Ph.D. dissertation, Dept. Aeronautics and Astronautics, MIT, Cambridge, MA, 2007. Available: http://dspace.mit.edu/handle/1721.1/42175

[63] N. Dulac *et al.*, “Using system dynamics for safety and risk management in complex engineering systems,” *Proc. 2005 Winter Simulation Conf.*, Orlando, FL, 2005, pp. 4-4.

[64] M. Ulrey and A. Shakarian, “System dynamics application in air traffic management: A case study,” In *Proc. 2008 ICNS Conf.,* Bethesda, MD, 2008.

[65] E. Hollnagel, *FRAM - the Functional Resonance Analysis Method: Modeling Complex Socio-Technical Systems.* Burlington, VT: Ashgate, 2012.

[66] EUROCONTROL, *A White Paper on Resilience Engineering for ATM,* Sept. 2012.

[67] EUROCONTROL, *Guidelines on the Systemic Occurrence Analysis Methodology (SOAM) (EAM 2 / GUI 8)*, Brussels. 2005. Available: http://www.skybrary.aero/bookshelf/books/275.pdf

[68] R. D. Alexander, “Using simulation for systems of systems hazard analysis,” Ph.D. dissertation, Dept. Comput. Sci., Univ. of York, York, UK, 2007. Available: http://www.cs.york.ac.uk/ftpdir/reports/2007/YCST/21/YCST-2007-21.pdf

[69] B. J. M. Ale *et al*, *Causal model for air transport safety: Final report,* Mar. 2, 2009. Available: http://www.nlr-atsi.nl/fast/CATS/CATS%20final%20report.pdf

[70] I. Svedung and J. Rasmussen, “Graphic representation of accident scenarios: Mapping system structure and the causation of accidents,” *Safety Sci.*, vol. 40, no. 5, pp. 397-417, Jul. 2002.

[71] C. H. Fleming *et al.,* “Safety assurance in NextGen,” NASA Langley Research Center, Hampton, VA, Rep. NASA/CR-2012-217553, Mar. 2012. Available: http://ntrs.nasa.gov/search.jsp?R=20120003581

[72] M. C. Consiglio *et al.*, “Impact of pilot delay and non-responsiveness on the safety performance of airborne separation,” in *8th Aviation Technology, Integration and Operations (ATIO) Conf.,* 2008 © AIAA. Available: http://hdl.handle.net/2060/20080040181

[73] Joint Planning and Development Office, *Capability Safety Assessment of Delegated Interval Management, unpublished.*

[74] S. A. Morello and W. R. Ricks, “Aviation safety issues database,” NASA Langley Research Center, Hampton, VA, Rep. NASA/TM-2009-215706, Apr. 2009. Available: http://ntrs.nasa.gov/search.jsp?R=20090015390

[75] N. Zelkin and S. Henriksen, ”L-band digital aeronautical communications system engineering: Initial safety and security risk assessment and mitigation,” NASA Glenn Research Center, Cleveland, OH, ep. NASA/CR—2011-216327, Jan. 2011. Available: http://ntrs.nasa.gov/search.jsp?R=20110005653

[76] N. Zelkin and S. Henriksen, "C-band airport surface communications system engineering: Initial high-level safety risk assessment and mitigation," NASA Glenn Research Center, Cleveland, OH, Rep. NASA/CR-2011-216325, Feb. 2011. Available: http://ntrs.nasa.gov/search.jsp?R=20110007900

[77] W. H. Rogers *et al.*, "Parametric modeling of the safety effects of NextGen terminal maneuvering area conflict scenarios," NASA Langley Research Center, Langley, VA, Rep. NASA/CR—2011-217082, Apr. 2011. Available: http://ntrs.nasa.gov/search.jsp?R=20110011504

[78] E. Ancel *et al.*, "NextGen Future Safety Assessment Game", in *MODSIM World 2010 Conf. Expo.,* VA, 2010, pp. 491-508. (NASA/CP-2011-217069/PT 2). Available: http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20110012078_2011012542.pdf

[79] B. J. Holmes *et al.*, "Development of complexity science and technology tools for NextGen airspace research and applications," NASA Langley Research Center, Hampton, VA, Rep. NASA/CR–2012-217580, Jun. 2012. Available: http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20120009939_2012010199.pdf

[80] J. W. Andrews *et al.*, "Safety analysis for advanced separation concepts," in *Proc.6th*^{t} *USA/Europe Air Traffic Management Research and Development Seminar,* MD, 2005, pp. 1-11. Available: http://www.ll.mit.edu/mission/aviation/publications/publication-files/ms-papers/Andrews_2005_ATM_MS-19317_WW-18698.pdf

[81] J. Shortle *et al.*, "Safety and sensitivity analysis of the advanced airspace concept for NextGen," in *Integrated Commun., Navigation and Surveillance Conf. (ICNS)*, Fairfax, VA, 2012, pp. O2-1 – O2-10.

[82] S. Borener *et al.,* "Design and development of an integrated safety assessment model for NextGen," *Amer. Soc. Eng. Manage. J.,* 2012.

[83] EUROCONTROL, "SESAR top-down systemic risk assessment," EUROCONTROL, France, Rep. D2.4.3-02 version 1.01, Oct. 2009. Available: http://www.episode3.aero/library/wp2/system_assessments/safety_assessment/d2.4.3-02-top-down-sesar-systemic-risk-assessment/E3-WP2-D2.4.3-02-REP-V1.01-sesar-top-down-systemic-risk-assessment.pdf

[84] R. E. Weibel and R. J. Hansman, "Assuring safety through operational approval: Challenges in assessing and approving the safety of systems-level changes in air transportation," MIT International Center for Air Transportation (ICAT) Dept. of Aeronautics & Astronautics, Cambridge, MA, rep. ICAT-2009-04, September 2009. Available: http://dspace.mit.edu/handle/1721.1/62970

[85] Federal Aviation Administration. *Safety Risk Management Guidance for System Acquisitions (SRMGSA) – Federal Aviation Administration Safety Management System (SMS) and Acquisition Management System (AMS) Guidance Document* (ATO-S 2008-12 version 1.5), Dec. 2008. Available: http://www.ipa.faa.gov/Displayblob.cfm?filename=SRMGSA_1.5.PDF

[86] Radio Technical Commission for Aeronautics, *Design Assurance Guidance for Airborne Electronic Hardware*, RTCA DO-254/ED-80, 2000.

[87] Department of Defense, *Department of Defense Standard Practice: System Safety (MIL-STD-882E),* 2012. Available: www.system-safety.org/Documents/MIL-STD-882E.pdf

[88] Radio Technical Commission for Aeronautics, *Software Considerations in Airborne Systems and Equipment Certification*, RTCA DO-178B, 1992.

[89] Radio Technical Commission for Aeronautics, *Guidelines for Communications, Navigation, Surveillance, and Air Traffic Management (CNS/ATM) Systems Software Integrity Assurance,* RTCA DO-278, 2002.

[90] Radio Technical Commission for Aeronautics, *Software Considerations in Airborne Systems and Equipment Certification*, RTCA DO-178C, 2011.

[91] E. Hollnagel, "Resilience – the challenge of the unstable," In E. Hollnagel et al., eds., *Resilience Engineering: Concepts and Precepts.* Burlington, VT: Ashgate, 2006.

[92] Y. Zhang, private communication, Dec. 9, 2012.

[93] S. H. Stroeve *et al.*, "Contrasting safety assessments of a runway incursion scenario: Event sequence analysis versus multi-agent dynamic risk modelling," *Rel. Eng. and System Safety,* vol. 109*,* pp. 133–149, Jan. 2013. Available: DOI http://dx.doi.org/10.1016/j.ress.2012.07.002

[94] M. H. C. Everdij, private communication, Nov. 27, 2012.

[95] Government Accountability Office, "Aviation safety: Additional FAA efforts could enhance safety risk management," GAO, Washington, DC, Rep. GAO-12-898, Sept. 2012. Available: http://www.gao.gov/assets/650/648110.pdf

[96] E. Perrin, private communication, Nov. 14, 2012.

[97] M. H. C. Everdij, private communication, Nov. 27, 2012.

Appendix A – Acronyms and Abbreviations

4D	Four-dimensional
A/C	Aircraft
ACO	Aircraft Certification Office
ADS-B	Automatic Dependent Surveillance Broadcast
AFS	Flight Standards Service
AIR	Aircraft Certification Service
Air-MIDAS	Air Man-Machine Integrated Design and Analysis System
ANSP	Air Navigation Service Provider
AOC	Airline Operations Center
AOV	Air Traffic Safety Oversight Service
ASDE	Airport Surface Detection Equipment
ASRS	Aviation Safety Reporting System
ATC	Air Traffic Control
ATS	Air Traffic Services
ATM	Air Traffic Management
ATO	Air Traffic Organization
ATSAP	Air Traffic Safety Action Program
ATS	Air Traffic Service
AVS	Aviation Safety
AVSMT	AVS Management Team
BBN	Bayesian Belief Network
CATS	Casual Model of Air Transport Safety
CCA	Common Cause Analysis
CDTI	Cockpit Display of Traffic Information
CIWS	Corridor Integrated Weather System
CNS	Communication, Navigation and Surveillance
ConOps	Concept of Operations
CONUS	Continental United States
CPDLC	Controller Pilot Data Link Communication
CRM	Crew Resource Management
D	Development
DCPN	Dynamically Colored Petri Nets
DHS	Department of Homeland Security
DNS	Domain Name Service
DO-	Document
DOC	Department of Commerce
DOD	Department of Defense
DOJ	Department of Justice
EA	Enterprise Architecture
EATMP	European Air Traffic Management Programme
EHS	Mode S Enhanced Surveillance
ELS	Mode S Elementary Surveillance
ESD	Event Sequence Diagram
EN	Enabler
ETA	Event Tree Analysis
EUROCONTROL	European Organization for the Safety of Air Navigation

EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
FAST	Future Aviation Safety Team
FCAPS	Fault, Configuration, Administration, Performance, and Security
FID	Flight Identification
FIM-S	Flight Deck Interval Management – Spacing
FIS-B	Flight Information Service-Broadcast
FMECA	Failure Modes Effects and Criticality Analysis
FRAM	Functional Resonance Analysis Method
FTA	Fault Tree Analysis
GAO	Government Accountability Office
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GUI	Graphical User Interface
HAZOP	Hazard and Operability study
HEART	Human Error Assessment and Reduction Technique
HERA	Human Error in ATM
HSMP	Hybrid-State Markov Processes
HSPD	Homeland Security Presidential Directive
HTA	Hierarchical Task Analysis
HTRR	Hazard Tracking and Risk Resolution
ICAO	International Civil Aviation Organization
IEEE	Institute of Electrical and Electronics Engineers
IRP	Integrated Risk Picture
ISAM	Integrated Safety Assessment Model
ISO	International Organization of Standardization
ITWS	Integrated Terminal Weather System
IWP	Integrated Work Plan
JPDO	Joint Planning and Development Office
JPE	Joint Planning Environment
KAS	Knowledge, Abilities, and Skills
LDAP	Lightweight Directory Access Protocol
MA-DRM	Multi-Agent Dynamic Risk Modeling
MIT	Massachusetts Institute of Technology
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NCI	Net-Centric Infrastructure
NEI	Net-Enabled Infrastructure
NEO	Net-Enabled Operations
NextGen	Next Generation Air Transportation System
NGIP	NextGen Implementation Plan
NLR	National Aerospace Laboratory
OI	Operational Improvement
OSA	Operational Safety Assessment
PBN	Performance-Based Navigation
PDARS	Performance Data Analysis and Reporting System
PDP	Piecewise Deterministic Markov Processes
PI	Policy Improvement
PIREP	Pilot Report
PKI	Public Key Infrastructure

PMA	Parts Manufacturing Approval
PNT	Positioning, Navigation, and Timing
QoS	Quality of Service
R	Research
R&D	Research & Development
RNAV	Area Navigation
RNP	Required Navigation Performance
RTCA	Radio Technical Commission for Aeronautics
SADT	Structured Analysis and Design Technique
SAE	Society of Automotive Engineers
SAFSIM	Safety in Simulation Method
SAS	Single Authoritative Source
Sec	Seconds
SD	System Dynamics
SESAR	Single European Sky ATM Research
SHEL	Software, Hardware, Environment, and Liveware
SIMMOD Pro	Simulation Model Professional
SLA	Service Level Agreement
SMS	Safety Management System
SOAM	System Occurrence Analysis Methodology
SoS	System of Systems
SRM	Safety Risk Management
SSA	System Safety Assessment
SSMT	System Safety Management Transformation
STAMP	Systems Theoretic Accident Model and Processes
STC	Supplemental Type Certificate
STI	Scientific and Technical Information
STPA	STAMP-based Analysis or System Theoretic Process Analysis
TBO	Trajectory-Based Operations
TFM	Traffic Flow Management
TM	Trajectory Management
TMA	Traffic Management Advisor
TMU	Traffic Management Unit
TOPAZ	Traffic Organization and Perturbation AnalyZer
TRACEr-Lite	Technique for the Retrospective and Predictive Analysis of Cognitive Error
TSO	Technical Standard Order
UAS	Unmanned Aircraft System
U.S.	United States
WG	Working Group

Appendix B – Elements of OI-0349 (Automation Support for Separation Management)

B.1. Enablers

EN-0039 UAS Detail Operation Concept

A policy decision will be made regarding how Unmanned Aircraft System (UAS) operations will be incorporated in the national airspace system. This decision includes standards for separation of UASs from other aircraft, procedures for UAS operations, requirements for onboard equipment, such as sense and avoid systems, and may encompass a set of standards for UASs with various performance and operational characteristics and equipage.

EN 0212 Parameter Driven Aircraft Separation Standards and Procedures

Separation management standards and procedures that allow Air Navigation Service Provider's (ANSP) and flight operators to safely manage separation using aircraft parameters and operating conditions. Safe separation standards and procedures will reflect aircraft capabilities, wake turbulence characteristics, operational geometries, and environmental conditions.

EN-0016 Separation/Trajectory Management Detail Operational Concept

The operational concept that defines the future roles of humans and automation to perform Separation and Trajectory Management (TM) functions in the NextGen environment. This concept will include roles for Air Navigation Service Providers (ANSP) as well as flight operator personnel. The concept will define the division of responsibilities that will guide the development of procedures and automation system requirements.

EN 0035 Separation Management Decision Support - Level 1

Separation Management Decision Support, Air Navigation Service Providers (ANSP) automated decision support tools that support the safe management and execution of separation procedures and standards in all airspace domains. This capability incorporates real-time information from ground-based and aircraft systems, and integrated trajectory management procedures and standards. These tools enhance NAS' ability to ensure that aircraft are safely separated from potential conflicts from other aircraft, wake turbulence, terrain, restricted airspace, and obstacles. Separation management is integrated with Trajectory Management, capacity and flow contingency management support tools using a net-centric infrastructure and system wide information management providing full situational awareness of all elements needed, such that potential conflicts can be automatically detected. These decision support tools will recommend and support the execution of conflict resolution with separation management being negotiated and delegated among ANSP and flight operations for all operations.

EN-1231 NextGen Enterprise Network – FAA

Within the Federal Aviation Administration (FAA) enterprise, NextGen information is managed and shared using a service-oriented enterprise network. As part of the overall NextGen enterprise network, this FAA-specific enterprise network provides internal services,

supports internal users, and exchanges NextGen information with non-FAA sources. Current plans envision this FAA enterprise network to operate on the FTI (FAA Telecommunications Infrastructure) with direction from the SWIM (System Wide Information Management) program. This enterprise network: (1) complies with NextGen minimum standards for network management and infrastructure/security services, (2) is deployed on an FAA physical network (links, switches, routers, etc.), (3) is tested and validated, and (4) is specific to FAA operational requirements and supports the delivery of FAA information services. As services are deployed, network managers must ensure that the enterprise network capacity and performance is sufficient to support the Service Level Agreements (SLAs) and quality of service (QoS) requirements associated with the information services. The availability date for this enabler reflects compliance with published NextGen standards.

EN-1015 Enterprise Network Management Standards

NextGen enterprise network management standards are authorized and published. All agency network management groups that participate in the NextGen information sharing environment must meet minimum standards. Network management is a continuous activity aimed at ensuring the successful operation of an enterprise network. A network management system typically consists of network managers assisted by automated tools running on and off the network. The International Organization of Standardization (ISO) Network Management Model establishes a framework for network management within and across network enclaves, business organizations, and integrated communities. The functional categories include Fault, Configuration, Administration, Performance, and Security (FCAPS) management. The goal of Fault Management is to recognize, isolate, correct and log faults that occur in the network. The goals of Configuration Management are to gather and store configurations from network devices (either locally or remotely), track changes which are made to the configuration, and to configure ('provision') circuits or paths through non-switched networks. The goals of Administration Management are to administer the set of authorized users by establishing users, passwords, and permissions, and to administer the operations of the equipment such as by performing software backup and synchronization. The goal of Performance Management (PM) is to enable the manager to prepare the network for the future and to determine the efficiency of the current network, using throughput, percentage utilization, error rates and response time's metrics to mange the network efficiency. The goal of Security Management is to control access to assets in the network, including such aspects as physical security of network equipment and boundary protection policies regarding firewalls, gateways, and other network connections. Network security policies must be continuously enforced. In addition to FCAPS, life-cycle management must be addressed for all network infrastructures (hardware, software, standards and protocols, etc.). Network designers and implementers must also factor into their plans the need for network expansion (new services, new users) and/or performance upgrades while maintaining continuous operations.

EN-1230 Enterprise Networking Governance Structure

A governance structure (a body with defined membership and processes) is established to develop and authorize common requirements related to enterprise networking that will be applied across agencies. The goal of this governance structure is to ensure cross-agency interoperability and standardization while minimally limiting agency flexibility in its implementation decisions. This governance group will publish cross-agency requirements regarding standards and protocols in areas such as enterprise network management, infrastructure, and information sharing.

EN-1229 Enterprise Networking Governance Model

This is the high-level governance model for guiding enterprise network implementations across agencies. This governance model will describe the governance structure (a body with defined membership and processes) that will define cross-agency requirements related to enterprise networks including network management, infrastructure, and information sharing.

EN-1016 Enterprise Networks Infrastructure Services Standards

NextGen enterprise network infrastructure services standards and protocols are authorized and published. All agency enterprise networks that participate in the NextGen information sharing environment must meet minimum standards. In a service-oriented enterprise network, infrastructure services support the management and transport of data within and across network enclaves, business organizations, and integrated communities in a standardized and common manner. These infrastructure services include Registry/Discovery and Message Mediation. The goal of the Registry/Discovery Service is to provide the Enterprise Service locations and protocol bindings that are available. Standards related to Registry/Discovery should address the service registration process, guidelines for registry content, a framework for Service Level Agreements (SLAs), and metadata repositories related to service registry entries. On the same theme as Registry/Discovery, the standards should also address the use of lower-level network organization protocols such as DNS and LDAP. The goal of Message Mediation is to provide mechanisms to support service invocation styles (e.g., publish/subscribe, request/reply) and data exchange protocols. It enables message routing including the structures and metadata supporting intelligent (e.g., content-based) routing and policy. The mediation function must provide messaging Quality of Service (QoS) including priority and response time for each transaction. Infrastructure services standards should also describe the monitoring and reporting mechanisms necessary to continuously assess the health of infrastructure services and assure proper operation.

EN-1043 Enterprise Networks Security Services Standards

NextGen enterprise network security services standards and protocols are authorized and published. All agency enterprise networks that participate in the NextGen information sharing environment must meet minimum standards. The goal of security services is to enforce security policies at the service and message level including providing authorization-based access to data and services (identity and role-based access control). Security services allow users to access the information they need, while securing classified/sensitive data from access by unauthorized persons and protecting networks from intended/unintended corruption by 'malicious' or hidden code. Security services ensure both publishers and subscribers can verify identities, authenticate themselves, and assert access privileges. Identification and authentication can be accomplished using services such as Public Key Infrastructure (PKI) services. Leveraging encryption, security services also ensure confidentiality and information integrity by guarding against unauthorized modification of data and services. Security services standards should also describe the monitoring and reporting mechanisms necessary to continuously assess the health of security services and assure proper operation.

EN-1271 Flight and Surveillance Information Services - FAA Group 1

This enabler provides the initial group of services for the Federal Aviation Administration (FAA) delivery of flight and surveillance information. Flight information includes flight plan data (aircraft identification, planned routes and times, etc.). Surveillance information includes current

aircraft track data (position and other real time characteristics) for the en route and surface domains. Clearance delivery and taxi status information is also available. These information services are implemented on the FAA's enterprise network, where they can be accessed by outside users (other agencies, third parties) via authorized gateways/portals. Service and infrastructure implementation must take into consideration the required bandwidth and quality of service (QoS).

EN-1025 Airport Surface Surveillance - Legacy ASDE-X

The Airport Surface Detection Equipment Model - 3/X (ASDE-3/X) provides integrated airport surface surveillance - via plot level fusion of radar technology, multilateration, Automatic Dependent Surveillance-Broadcast (ADS-B), & aircraft equipment. Fused track plot data is then placed on Air Navigation Service Provider (ANSP) tower display. This is a closed non-network system. Provides aircraft and other ground vehicle positions and movement on the surface of the airport.

EN-1251 Information Sharing Standards: Flight and Surveillance Information

The net-centric governance structure publishes authorized standards for providing and exchanging flight and surveillance information across the Net-Centric Infrastructure (NCI) of the NextGen enterprise. These standards define the technical vocabulary, schemas, metadata, business processes, and related specifications essential to the net-centric exchange of flight and surveillance information. Flight and surveillance information includes: flight plan data, surveillance for airborne and surface traffic (cooperative and non-cooperative), clearance delivery, and taxi status. These standards enable services to share information in a consistent and uniform way.

EN-2680 Methodologies and Algorithms for Weather Assimilation into Decision-Making

This enabler provides guidance, methodologies, and algorithms for weather assimilation into decision-making. This is accomplished through initial, crosscutting, foundational research such as: translation of weather's impact on operations, operational metrics development, determination of NextGen relevant weather information, basic mathematical research into optimization methodologies, operational research analysis, techniques for the presentation of probabilistic information to humans and automation, characterization of hazardous weather phenomena (e.g., estimation of aircraft-specific weather hazard levels, pilot likelihood to deviate, permeability of weather), benefits pool estimation, and weather forecast verification. This near-term research will likely produce more immediately useable results for weather assimilation for the en route and terminal domains, because of the current maturity of research in en route weather conflict prediction and resolution; arrival/departure separation standards due to wake vortex turbulence; and ceiling and visibility impacts on airport arrival rates. Another reason these capabilities are anticipated in the near-term is that the look-ahead time for the required weather is relatively short, resulting in levels of weather uncertainty that can be more easily addressed. Some early, less sophisticated results in the assimilation of weather in the Traffic Flow Management (TFM) domain and surface operations may also be achieved.

EN-0301 Performance-Based Separation Standards and Procedures

Performance-Based procedures and standards allow the Air Navigation Service Provider (ANSP) and Flight Operators to conduct reduced oceanic, en route, and terminal separation,

such as: - 3-mile en route separation - alternatives evaluation and selection - 3-mile en route separation procedures - non-mosaic display - 5-mile non radar airspace separation procedures - Variable wake-based separation standards and procedures - Reduced oceanic separation standards and procedures The en route procedures provide accurate aircraft positional information to pilots and ground-based controllers enabling the reduction of separation to 3 miles, or 5-mile reduction which accommodates new larger aircraft and collision or wake turbulence encounter risk limits. Space-based data and voice communication provides direct controller-pilot communications enabling alternative trajectory operations.

EN-2010 NextGen 4D Weather Cube Information - Manual SAS Selection

The 4D Weather Data Cube, with non-automated Single Authoritative Source (SAS) selection, will provide the Initial Operational Capability. Weather analyses, diagnoses and forecasts are available to all users over a network-enabled infrastructure. Weather information for this level will include, at a minimum, winter weather, convection, icing, turbulence, and restrictions to visibility. This enabler includes development of business rules and capabilities to process weather observations and multiple forecast capabilities into a single, authoritative, four-dimensional (4D) weather source available across varied space and time scales. The initial SAS may be limited to a subset of aviation weather parameters (e.g., convection, turbulence) and may be determined using objective data such as verification results for various forecast alternatives through a human-based selection process.

EN 1273 NextGen Weather Information Services - FAA Group 1

This enabler provides the initial group of services for the Federal Aviation Administration (FAA) delivery of weather information including: Pilot Weather Reports (PIREPs), Integrated Terminal Weather System (ITWS) products, and Corridor Integrated Weather System (CIWS) products. ITWS and CIWS focus on convective weather near airports and en route, respectively. These information services are implemented on the FAA's enterprise network, where they can be accessed by outside users (other agencies, third parties) via authorized gateways/portals.

EN-2080 Network-Enabled User-Defined Weather Information Request Function

The Weather Request function will support trajectory and volumetric based retrievals from the 4D Weather Data Cube and its Single Authoritative Source (SAS). Weather Request enables user defined requests (i.e., querying) for weather information (e.g., weather along flight path) tailored to the operational need. Users obtain the specific information they require, rather than being provided volumes of information from which they need to locate and interpret the information they require. Weather Request also enables the Weather Translation function.

EN-2700 Weather Information Regulatory Structure

This new weather regulatory structure is necessary to accommodate NextGen weather capabilities and technological advancements. It will identify regulations and guidance material (Advisory Circulars, etc.) that may require revision to support the use of the NextGen 4D Weather SAS. It will address numerous policy issues such as: How will weather information from the network-enabled 4D Weather Data Cube address today's regulatory requirements? How will information in the 4D Weather Data Cube be certified for use?

EN-1234 NextGen Enterprise Network – DOC

Within the Department of Commerce (DOC) enterprise, NextGen information is managed and shared using a service-oriented enterprise network. As part of the overall NextGen enterprise network, this DOC-specific enterprise network provides internal services, supports internal users, and exchanges NextGen information with non-DOC sources. This enterprise network: (1) complies with NextGen minimum standards for network management and infrastructure/security services, (2) is deployed on a DOC physical network (links, switches, routers, etc.), (3) is tested and validated, and (4) is specific to DOC operational requirements and supports the delivery of DOC information services. As services are deployed, network managers must ensure that the enterprise network capacity and performance is sufficient to support the Service Level Agreements (SLAs) and Quality of Service (QoS) requirements associated with the information services. The availability date for this enabler reflects compliance with published NextGen standards.

EN-2050 Information Sharing Standards: Weather Information

The standards that allow weather data to be universally transported on a network-enabled infrastructure and used by a variety of automated support systems are developed and guide the implementation of the network-enabled capability. Weather data include the dissemination of consolidated observation and forecast data as well as the collection and control of sensor data.

EN-2040 NextGen Net-Enabled Operations Virtual 4D Weather Data Cube Governance Structure

A governance structure is established, based on existing governance models, to manage the development, authorization, standards, policy, and certification of the NextGen Net-Enabled Operations (NEO) Four Dimensional (4D) Weather Data Cube and to provide a Single Authoritative Source (SAS) of current and forecasted weather information. The governance structure will define: NextGen 4D Weather Data Cube content, business rules, boundaries with the national weather information infrastructure, the general public's level of participation, categories of publisher/subscribers, and roles of foreign entities. It will also provide the mechanism, criteria, and policy for accepting/approving subscribers/providers, and establish the delineation between state of the atmosphere information and translated weather constraint information.

EN-2710 NextGen Net-Enabled Operations 4D Weather Data Cube Governance Models

This is the high-level Governance Model for all of aviation weather and includes: delineating the boundaries of private and public sector weather information; defining inter-agency weather roles and responsibilities; and arbitrating inter-agency financing of NextGen weather. There are two weather governance systems. The first is for civil weather services, which is free and open to the world. The second is for aviation weather system management (i.e., 4D Weather Data Cube), which needs to be secure and protected. Within the aviation weather system there are two distinct governance groups: NEO for weather dissemination and NextGen Weather for weather information. Each of these governance groups will build a governance framework to support the network-enabled 4D Weather Data Cube, which jointly will protect weather data and make it available.

EN-2260 Integrated Network-Enabled Weather Observation System

Develop an overall strategy and implementation plan to define the capabilities of an adaptive, integrated network of ground, air and satellite weather sensors. This includes the research and acquisition strategy needed to support the plan. This plan will result in the elimination of independent and redundant plans, strategies, and acquisitions. Integration of ground, airborne and satellite weather observation information in real time (includes hardware, software and interfaces) enables the creation of the initial single authoritative source of current weather information

EN-2220 Network-Enabled Weather Observation System - Ground-Based

Network-enabled ground-based sensor system is the initial observation sensor system, which includes connectivity to the net-centric environment (i.e., hardware, software and interfaces) and supports the collection of ground-based observations.

EN-2230 Network-Enabled Weather Observation System - Airborne - Major Carriers

This initial sensor system builds upon current airborne sensor systems. It supports the collection of observations (e.g., turbulence, icing, winds, temperature, and water vapor) from major passenger, regional passenger, and package carriers. The data is network enabled by ground systems. Other airborne observations will be used if they are available in this timeframe.

EN-2240 Network-Enabled Weather Observation System – Satellites

Network-enabled space-based sensor system is the near-term observation sensor system, which includes connectivity to the net-centric environment (i.e., hardware, software and interfaces) and supports the collection of space-based observations.

EN-2060 Aviation Weather Information System - Network-enable Existing Systems

Network-enable multi-agency legacy system functions (e.g., Federal Aviation Administration (FAA), Department of Defense (DOD)). Current point-to-point communications and unique processing of weather information (e.g., Weather and Radar Processor, Integrated Terminal Weather System) are network-enabled to support legacy display systems. Following this weather processor migration, Air Traffic Management (ATM) applications, procedures, and operational concepts are redirected to the NextGen Net-Enabled virtual Four-Dimensional (4D) Weather Cube. Stakeholders benefit from reduced cost to acquire weather information, a common weather picture, and access to the same weather information available to all stakeholders.

EN-2410 Weather Forecasts - Consolidated Convective Storm

NextGen's initial predictive models and current weather observations are fused/blended to provide a consolidated convective storm diagnosis and forecast that is available to users over a network-enabled infrastructure. This capability will include forecasts for the Continental United States (CONUS) 0-4 hour timeframe.

EN-2420 Weather Forecasts - Consolidated Icing

NextGen's initial predictive models and current weather observations are fused/blended to provide a consolidated icing diagnosis and forecast that is available to users over a Network-Enabled Infrastructure (NEI). This capability will include forecasts for the Continental United States (CONUS) 0-12 hour timeframe.

EN-2430 Weather Forecasts - Consolidated Turbulence

NextGen's initial predictive models and current weather observations are fused/blended to provide a consolidated turbulence diagnosis and forecast that is available to users over a network-enabled infrastructure. This capability will include North America from 10,000 feet to FL450, 0-18 hours, updated hourly, and will forecast clear air and mountain wave turbulence.

EN-2440 Weather Forecasts - Consolidated Ceiling and Visibility

NextGen's initial predictive models and current weather observations are fused/blended to provide a consolidated ceiling and visibility diagnosis and forecast that is available to users over a network-enabled infrastructure. This capability will include 1) Continental United States (CONUS) 0-12 hours, updated hourly (diagnosis every 5 minutes) and 2) a high-resolution product around selected terminal areas.

EN-2520 Weather Forecasts - Consolidated Winter Storm

NextGen's initial predictive models and current weather observations are fused/blended to provide a consolidated winter storm diagnosis and forecast that is available to users over a Network-Enabled Infrastructure (NEI). This capability will include forecasts for the Continental United States (CONUS) 0-4 hour timeframe.

B.2. Development Activities

D-0520 Airport Information Architecture

Development of best practices and planning architectures for multiparty (including public and community involvement) airport development actions, supporting implementation by airport operators and communities.

D-1200 Guidance for Trajectory-Based Procedures

Development of trajectory-based procedures to support a national policy decision on liabilities related to the shift in separation responsibility from air traffic service providers to flight operators as well as from humans to automation.

D-0830 Trajectory Negotiation Protocols for Air and Ground Information Architectures

Development of trajectory negotiation protocols, including appropriate authorization/hand shake definitions to secure aircraft/ground ops exchange of information, supporting aircraft and ground information architectures.

D-2135 Air and Ground Separation Management Architecture

Development of air/ground separation management architectures that can satisfy NextGen's increased capacity and safety requirements.

D-0260 Development of NextGen Interagency NCI Requirements

Development of NextGen interagency Net-Centric Infrastructure (NCI) requirements, including but not limited to: infrastructure equipment and platforms (in generic terms), information sharing strategies, exchange protocols, and metadata standards. This focuses on high-level requirements for the low-level network; it does not include security and information services addressed in more detail by other development items.

D-1070 Development of NextGen Interagency Net-Centric Security Requirements

Development of information security plans and guidelines to support information sharing among NextGen Partners that include security policies, protocols, performance measure criteria, assessment evaluation procedures, as well as certification, verification and validation methodologies of authorized users and providers of secured and non-secured information. This is important to support agency policy decisions about sharing information.

D-2194 Net Enabled Operations Prototype Development/Evaluation

Development of the Net-Enabled Operations (NEO) Spiral 1 joint project is a prototype development/evaluation effort which connects and builds outward from legacy air traffic and air security systems. NEO spiral 1 will be conducted in four 90 day engineering activities intended to determine how a NextGen NEO system should perform. This is an operational risk reduction measures that will develop expanded interagency collaboration tools and lead to future targeted implementations of NextGen NEO capabilities.

D-0260 Development of NextGen Interagency NCI Requirements

Development of NextGen interagency Net-Centric Infrastructure (NCI) requirements, including but not limited to: infrastructure equipment and platforms (in generic terms), information sharing strategies, exchange protocols, and metadata standards. This focuses on high-level requirements for the low-level network; it does not include security and information services addressed in more detail by other development items.

D-1070 Development of NextGen Interagency Net-Centric Security Requirements

Development of information security plans and guidelines to support information sharing among NextGen Partners that include security policies, protocols, performance measure criteria, assessment evaluation procedures, as well as certification, verification and validation methodologies of authorized users and providers of secured and non-secured information. This is important to support agency policy decisions about sharing information.

D-1220 Development of Weather Hazard Severity Indices

Development of severity indices for turbulence, convection, icing, and other aviation weather hazards. These indices will help identify the impacts of weather on specific aircraft types and configurations that will be crucial during collaborative decision-making.

D-2113 Operating Procedures for Human Forecasters using Automated Systems

Development of operating procedures outlining the role of human forecasters augmenting automatically generated Four-Dimensional (4D) weather grids.

D-0480 Reduced Oceanic Separation Standards and Procedures

Development of non-radar 30 mile lateral separation standards and procedures for use in Oceanic airspace.

D-0490 5nm Non-Radar Separation Standards and Procedures

Development of 5 mile non-radar longitudinal separation standards and procedures.

D-0920 Advanced Scheduling Decision Support Tool Enhancements

Development of en route and advanced terminal scheduling tool requirements, in the form of Traffic Management Advisor (TMA) improvements, along with site adaptations and operational use procedures. This includes research to generate time-based schedules for aircraft executing NextGen arrival procedures.

D-2127 3D RNAV/RNP Procedures

Development of initial Three Dimensional (3D) Area Navigation/Required Navigation Performance (RNAV/RNP) procedures for aircraft operator implementation.

D-2117 Network-Enabled Weather Data Standards

Development of a virtual, authoritative, net-centric Four Dimensional (4D) weather information system that provides information tailored to Air Traffic Management (ATM) procedures, including routine (diagnostics and forecasts) and real-time hazardous weather information to support an implementation decision on the network-enabled 4D Weather Cube.

D-2179 Enhanced Ground-Based Weather Sensors

Development of NextGen ground-based sensors that will be installed/modified at specified airports and other locations to provide weather and environmental observations.

D-2191 Enhanced Airborne-Based Weather Sensors

Development of NextGen airborne sensors that is installed/modified on aircraft and unmanned aerial systems to provide weather and environmental observations.

D-0840 Weather Forecast Assessment Verification System

Development of a real-time verification system that quantitatively assesses the accuracy, reliability, quality, and timeliness of weather forecasts (e.g., probabilistic information) to support collaborative Air Traffic Management (ATM) decision-making for trajectory-based and flexible terminal operations.

D-0850 Network-Enabled Weather Information System

Development of a virtual, authoritative, net-centric four-dimensional weather information system that provides information tailored to Air Traffic Management (ATM) procedures, including routine (diagnostics and forecasts) and real-time, hazardous weather information.

B.3. Research Activities

R-1190 Applied Research on Certification Methods, Requirements, and Standards for UASs

Applied research on safety certifications for control systems, sense and avoid capabilities, collision avoidance capabilities, and emergency procedures as they apply to Unmanned Aerial Systems (UAS).

R-1370 Applied Research on the Operational Concept for UASs in Trajectory-Based Airspace

Applied research on Unmanned Aircraft System's (UAS) operational and air-ground systems integration into trajectory-based airspaces to support alternative selection and regulation decisions on UAS access and transparency requirements.

R-1230 Applied Research on Weather and Wake Impacts for En Route Operations

Applied research to incorporate weather and wake impacts into reduced en route separation standards and overall en route operational procedures.

R-0600 Applied Research on Assessing and Predicting Wake Severity

Applied research to assess and predict the severity of aircraft wake encounters based on aircraft parameters and wake encounter geometry.

R-2126 Applied Research on Airframe Designs to Accelerate Wake Vortex Decay

Applied research on airframe design technologies that accelerate wake vortex decay.

R-2114 Applied Research on Improved Weather Sensing and Forecasting Models

Applied research on improved models for weather sensing and forecasting relevant to NextGen decision-making during convective and winter weather, turbulence, icing, clouds, visibility, volcanic ash dispersion, space weather, environmental factors (noise, emissions and hazardous release dispersion, upper atmospheric climate effects), and wake vortices

R-1620 Applied Research on Aircraft-Based CNS Technologies in Self-Separation Airspace

Applied research on initial traffic spacing management alternatives in congested en route airspace to support an alternative selection on Trajectory Management, merging, spacing and metering.

R-1460 Applied Research on Common Surface Automation Platform

Applied research for a common surface automation platform, networking and display systems to support cost-effective automated and integrated arrival/departure decision support systems and information technology infrastructure in the tower environment.

R-1060 Applied Research on NextGen Team Size Optimization

Applied research to understand NextGen optimal team sizes and skill set compositions to support staff management and facility design.

R-2112 Applied Research on Weather Integration into NextGen Decision Making

Applied research on the most effective methodologies, algorithms, and tools for the integration of weather information into NextGen decision-making such as: translation of weather's impact on operations, operational metrics development, determination of NextGen relevant weather information, basic mathematical research into optimization methodologies, operational research analysis, techniques for the presentation of probabilistic information to humans and automation, characterization of hazardous weather phenomena (e.g., estimation of aircraft-specific weather hazard levels, pilot likelihood to deviate, permeability of weather), and benefits pool estimation

R-0370 Applied Research on Advanced Scheduling Concepts in Congested Terminal Airspace

Applied research on traffic spacing management for transition, arrival, and departure operations supporting high-throughput delivery of aircraft to the runway threshold and high-throughput departure operations, including capacity benefits and potential increased arrival/departure rates.

B.4. Policy Issues

PI-0006 Balance of Human vs. Automation

Policies should be explored to determine the balance and trade-offs between automation and human participation in traffic management. Improper functional allocation between automation and human can decrease efficiency, effectiveness, and safety. Decisions related to this allocation should consider the adequate level of human involvement that will be required and the level of reliance on automation that will be acceptable to the flying public.

PI-0115 NextGen Safety Assessment/Certification - Synchronization of Aircraft and ANS Capabilities

The aircraft and Air Navigation Service Provider (ANSP) systems envisioned for NextGen are technically innovative, highly sophisticated, and interdependent. Many NextGen improvements require the synchronized implementation of these interdependent and integrated yet separate aircraft and ANSP systems. To support the most efficient implementation of these improvements yet address all safety issues, NextGen operational improvements should be assessed as integrated capabilities. A system safety approach should be used that considers elements such as procedures, backup capabilities and the interrelationships of all systems used to accomplish the operational improvement. Rather than separate assessments and certification

of individual systems, the safety assessment and certification process will include an approach incorporating the integrated use of aircraft and ANSP systems.

PI-0116 NextGen Safety Assessment/Certification - Standards and Tools

The systems envisioned for NextGen will be technically innovative and highly sophisticated, permitting aircraft to operate in new and more flexible ways, and resulting in changing roles for operators. New safety assessment standards, methodologies, and verification and validation tools must be developed for application to NextGen capabilities and requirements that cannot be adequately assessed through existing processes. Techniques and technologies to identify emergent risks must be developed.

PI-0110 International Commercial Space Operations

Policy mechanisms need to be developed to ensure that U.S. commercial space operations are allowed to depart from U.S. spaceports and land in spaceports located in foreign countries. These policies should ensure that launches originating in foreign countries and destined for the U.S. do not pose public safety or national security risks.

PI-0022 GPS Policy to Support Civil NextGen PNT Requirements

A great deal of reliance is being placed on the Global Positioning System (GPS) for NextGen Positioning, Navigation, and Timing (PNT) services for Communications, Navigation, and Surveillance (CNS). The GPS system may not meet civil requirements. Current Department of Defense (DOD) minimum GPS performance guarantees do not provide sufficient performance to meet civil requirements, without augmentation. Despite actual, demonstrated performance that exceeds the current commitment; civil reliance on the system can only rely on the U.S. Government commitment specified in the GPS standard performance service specification. Policies should be reviewed to ensure that GPS performance guarantees support requirements in a cost-effective manner for both service provider and user. Reliance on foreign Global Navigation Satellite System (GNSS) should be considered as part of this review (see PI-0075).

PI-0024 Secure Information Exchange

1) Develop policies to define (an) organization(s) that will maintain ownership of aviation information. 2) Develop policies to address handling current and archived data to protect privacy and proprietary information; establish mechanisms for protecting competitive information; create an oversight body with jurisdiction and responsibility over stakeholder data; and delegate certification responsibility. 3) Develop streamlined U.S. and international regulatory/policy coordination, through International Civil Aviation Organization (ICAO) and/or other bilateral/multilateral partnerships, related to secure information exchange of aviation related information, including access rules and governance. Secure exchange of information includes access controls, trust relationships, associated policies and mechanisms to provide appropriate access to information by authenticated users. Information content may be impacted by legal ramifications, proprietary preference, and civil liberties concerns and policies. Top Secret, Secret, Controlled but Unclassified, and industry proprietary information must remain protected in the net-centric NextGen. Cross-domain (e.g., Multi-Level Security Exchange/Gateway Capability) secure communication is a critical feature of data availability. The policy domains constituting NextGen include, but are not necessarily limited to, the following: FAA, Department of Defense (DOD), Department of Commerce (DOC), Department of Justice (DOJ), Department

of Homeland Security (DHS), National Aeronautic and Space Administration (NASA); state, local, and tribal law enforcement and emergency responders; airline operating companies; General Aviation (GA) facilities; commercial air traffic communication providers; foreign civil aviation authorities and ICAO.

PI-0120 PNT Performance Requirements

Develop policy to determine which backup Position, Navigation and Timing (PNT) services constitutes "critical" aviation infrastructure applications according to Presidential directive. Homeland Security Presidential Directive (HSPD) 7 states: "In accordance with U.S. Space-Based [PNT] Policy, the Secretary of Transportation, in coordination with the Secretary of Homeland Security, will develop, acquire, operate, and maintain backup [PNT] capabilities that can support critical transportation, homeland security, and other critical civil and commercial infrastructure applications within the U.S., in the event of a disruption of the Global Positioning System (GPS) or other space-based PNT services...." Moreover, develop streamlined U.S. and international regulatory/policy coordination, through the International Civil Aviation Organization (ICAO) and/or other bilateral/multilateral partnerships, in order to manage standardization and/or compatibility changes in PNT performance requirements. This is meant to address domestic and foreign aircraft within U.S. airspace and across international airspace boundaries. (e.g., Performance requirements for Required Navigation Performance [RNP] 0.1 should be consistent among states and operational approval in one state should be accepted by other states; the same should be true for Automatic Dependent Surveillance-Broadcast [ADS-B] performance requirements.)

PI-0009 National Integrated Surveillance Plan

Policies are needed to define the security levels, criteria and approval processes that will guide the sharing of complementary cooperative and non-cooperative surveillance data among public and private entities. These should address content attributes such as accuracy, timeliness, identification and authorization. At a minimum, Department of Defense (DOD), Department of Homeland Security (DHS), Department of Transportation / Federal Aviation Administration (DOT/FAA) and operators must collaborate on policies regarding the collection and distribution of surveillance data and requirements for data security, network security and access requirements. Associated policies must then be developed to ensure that each user is able to access complete, accurate and timely surveillance information to satisfy their operational requirements.

PI-0110 International Commercial Space Operations

Policy mechanisms need to be developed to ensure that U.S. commercial space operations are allowed to depart from U.S. spaceports and land in spaceports located in foreign countries. These policies should ensure that launches originating in foreign countries and destined for the U.S. do not pose public safety or national security risks.

PI-0087 Weather Information Policy - Use of Single Authoritative Source in ATM Decisions

A policy should be established to ensure that the NextGen Four-Dimensional (4D) Weather Cube Single Authoritative Source (SAS) is the required source of weather information for pilot and air traffic management (ATM) decisions. Additionally, such policy must ensure that weather

information in the Cube is equally and readily available to all airspace participants under open and unrestricted data rights.

PI-0089 Weather Avoidance Decision Making Responsibilities

1) In an environment where weather information is more readily available to the pilot in the air via net-centric communications and/or Flight Information Service-Broadcast (FIS-B) what is the requirement and the nature of controller dispensed weather advisories? Providing additional weather products does not make the controller more effective in providing weather advisories without enhanced translation. When these can be translated automatically into traffic/trajectory impacts should the user subscribe to an advisory service or should the controller retain that voice requirement. What is the concept of advisory services in a digital environment? 2) In the future of digital communications, the Airport Operations Center (AOC), Pilot, controller and Traffic Management Unit (TMU) can be actively linked in weather related flow and trajectory reroutes. How will digital communications change the manner in which these objectives are accomplished now that all actors can be linked into the data conversation versus the voice only limitations on their current interactions? The responsibilities are the same, but limitations on executing the responsibilities real-time have been relieved.

PI-0086 Weather Information Policy - Global Harmonization

Develop streamlined U.S. and international standards and guidelines, through International Civil Aviation Organization (ICAO) and other international aviation, meteorological governing bodies, and bilateral/multilateral mechanisms regarding standards for weather information provided by all states. Weather information in the form of meteorological variables that are observed or forecasted (e.g., storm intensity, echo tops, etc.) must be translated into information that is directly relevant to NextGen users and service providers, such as the likelihood of a flight deviation, airspace permeability, and capacity. Global coordination is needed to establish common standards for weather information provided by all nations.

PI-0088 Federal vs. Private Role In Weather Services

NextGen envisions a single, authoritative source for aviation weather and a common weather picture for all air transportation users. Eventually this picture would be incorporated into decision support tools available to automation, controllers and pilots. Policy should be developed to determine the roles and responsibilities of government, private, and academic participants in the nation's weather enterprise to take full advantage of their capabilities to meet NextGen weather requirements.

OI-0349 Automation Support for Separation Management

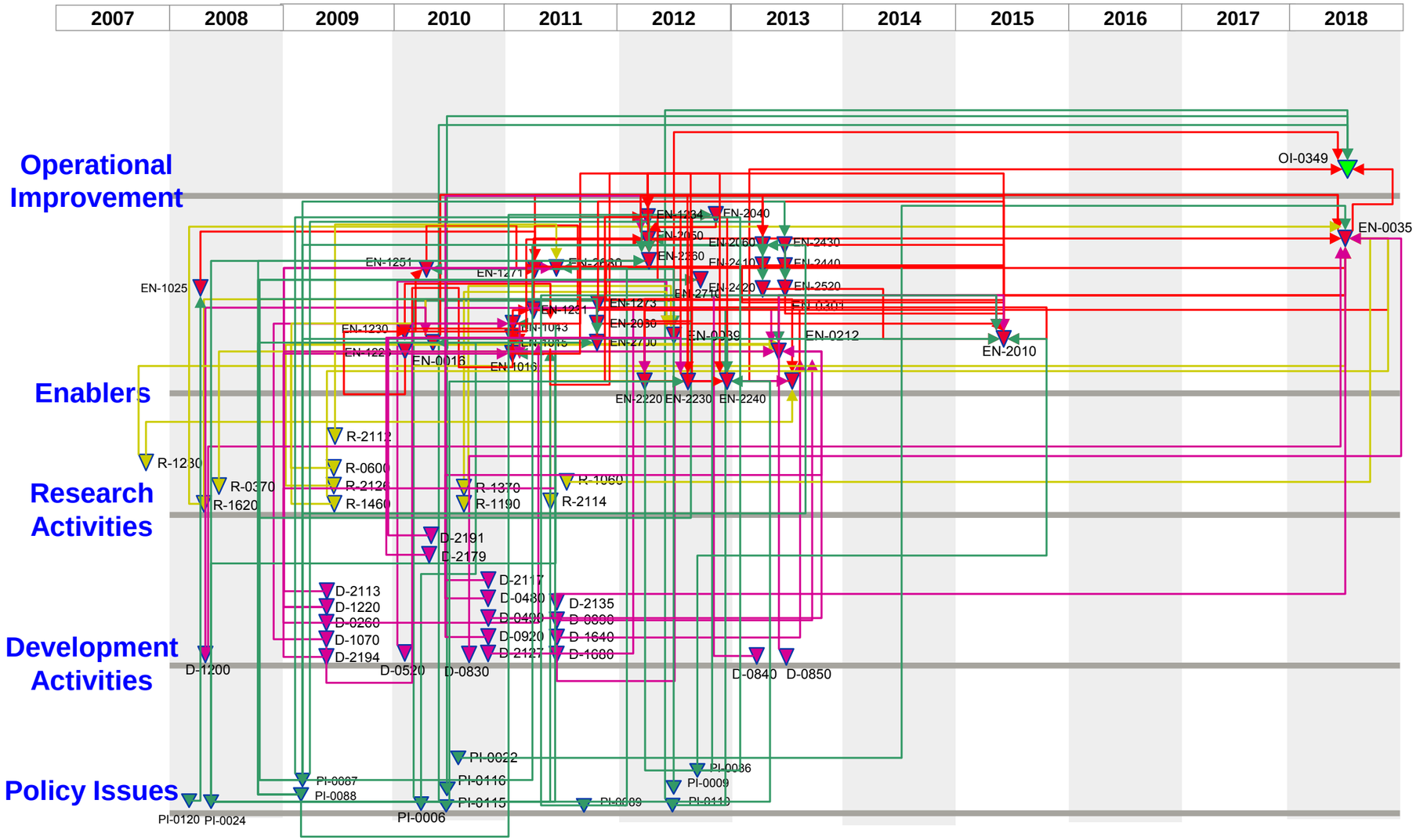


Figure C1. Relationship among OI-0349 and Its Supporting Elements

Appendix D – Simple and Complex Versions of an OI-0349 Scenario

D.1. Simple Version of the Scenario

This simple version of the scenario features departures from two different runways at a single airport with common Standard Instrument Departures being conducted from a merge point. Instead of the conventional approach in which the tower controller might regulate the takeoff spacing to try to assure longitudinal separation at the merge point without excessive use of tactical instructions by the approach controller after the aircraft take off, airborne surveillance in the form of flight deck based interval management for spacing (FIM-S) is used to allow the flight crew of the trailing aircraft to regulate speed and potentially takeoff interval to achieve the designated spacing interval by the time the lead aircraft reaches the merge point and then maintain that spacing until a termination point on the common route. BA123 has already received a departure clearance indicating use of runway 090R and then via FACTS and BTG to the BOILS departure.

While the aircraft are still taxiing to their respective runways, clearance delivery sends an FIM-S instruction to BA123 using CPDLC. The instruction clears BA123 to achieve and maintain 90 seconds spacing on BA789 who will depart on 09L via BLAKO and YKM to the BOILS departure (see Figure D1). The spacing is to be achieved by BOI and then maintained until SLC. The crew of BA123 loads the data into the FIM-S system and accepts the clearance. The crew of BA123 has intermittent contact with BA789 on the surface map traffic display during the taxi, and a solid contact as both aircraft reach the runway end. The FIM-S system monitors BA789 observing that data quality requirements for conducting FIM-S are met and, based on wind and temperature forecasts, assumptions about BA789's climb performance and speed, and the relative lengths of the two aircraft's departure paths between their respective runways and BOI, estimates that BA123 must take off 38 seconds after BA789. This initial interval would allow BA123 to fly its planned climb profile and speed schedule with no need to adjust. However, the crew understands that a number of factors can change the speed requirements.

BA123 is cleared for takeoff position on runway 09R as BA789 applies thrust for takeoff on runway 09L. The tower controller gives BA123 a 45 second runway hold window to allow for adjustment for the FIM-S procedure, and BA123 is able to apply thrust within a few seconds of the ideal predicted interval. No FIM-S speed guidance is presented to the flight crew during the takeoff phase; only when the aircraft reaches thrust reduction altitude does the FIM-S system regain its active state and present speed guidance.

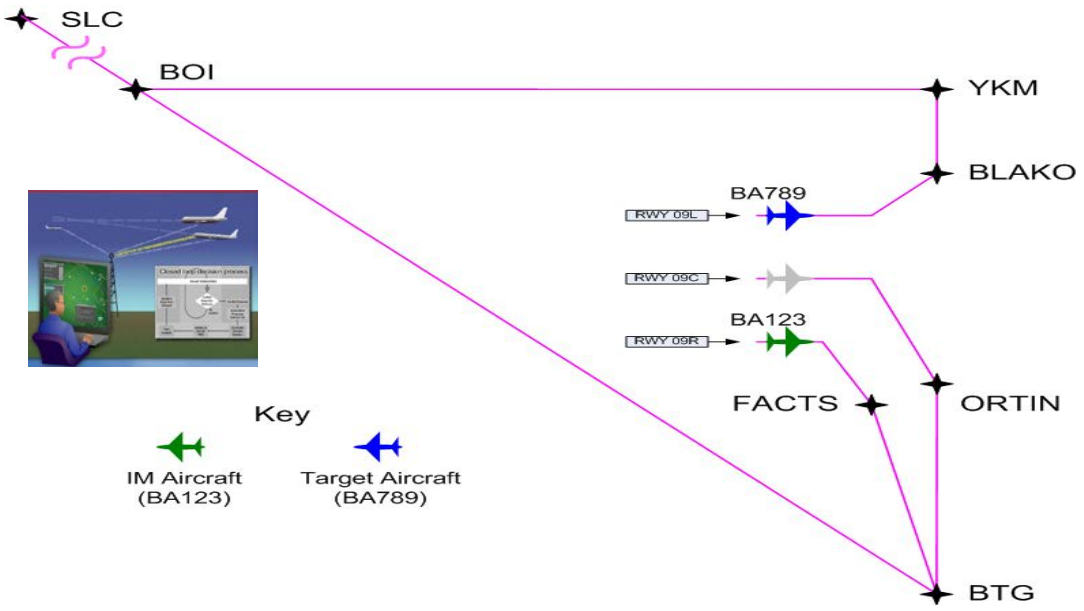


Figure D1. Simple Version of the Scenario (A)

Once the FIM-S system becomes active and speed guidance is provided, the crew responds to the guidance and informs the approach controller. While the aircraft remains below 10,000 feet msl, speed guidance is restricted to 250 KCAS or to the minimum speed for the aircraft model at high weight. By this time, BA789 has passed through 14,000 feet and has been handed off to Center. BA123 passes through 10,000 feet as it sequences BTG, and the displayed speed guidance increases to 327 kt. The guidance is fed to the aircraft's automation, and the pitch attitude of the aircraft changes to expedite the acceleration while still maintaining a rate of climb of more than 500 ft/min (see Figure D2).

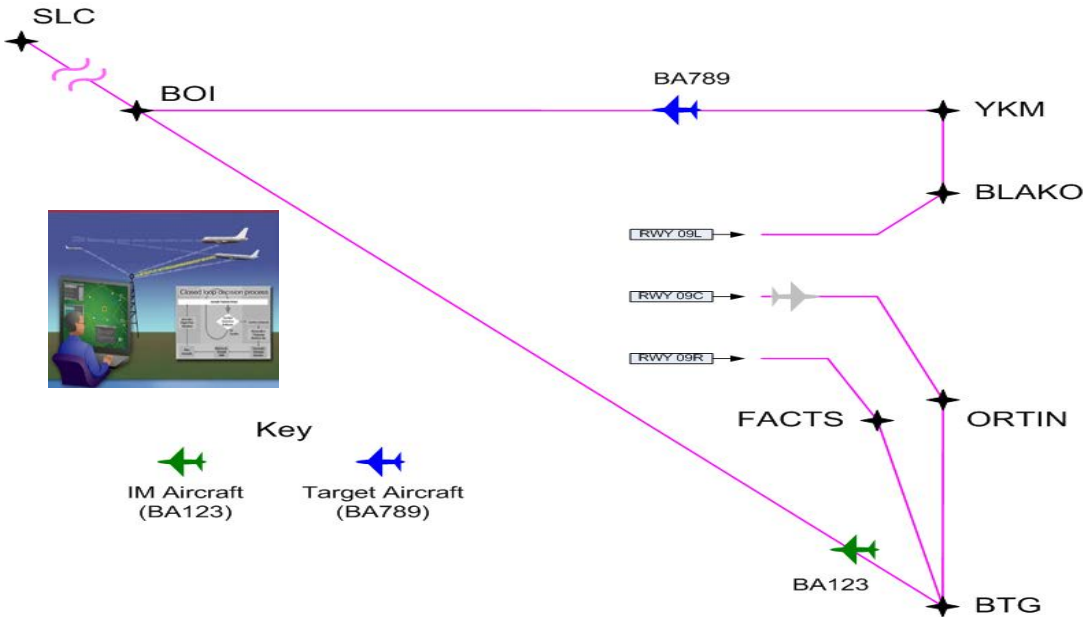


Figure D2. Simple Version of the Scenario (B)

From this point on, the FIM-S equipment continues to provide speed guidance to the flight crew of BA123 and to the aircraft's automation. The flight crew monitors the changes in speed guidance for acceptability and also for the continuing feasibility of achieving the cleared spacing value by the time the aircraft arrives at BOI. The crew also ensures that no failures are affecting the FIM-S operation. The arrivals controller monitors the operation to ensure that separation issues do not arise despite the fact that the lead aircraft has departed the sector. On reaching approximately 14,000 feet, the flight crew of BA123 switches frequency to Center and informs the controller that the FIM-S operation is ongoing. The Center controller assumes the task of monitoring the operation to assure separation.

When BA789 reaches BOI, the BA123 has 88 seconds to run before reaching BOI, and it is almost 9 NM behind BA789 and that distance is increasing (see Figure D3). The first FIM-S goal, that of achieving the assigned interval within tolerances by the achieve-by point (BOI), has been accomplished. The FIM-S system enters the 'maintain' mode.

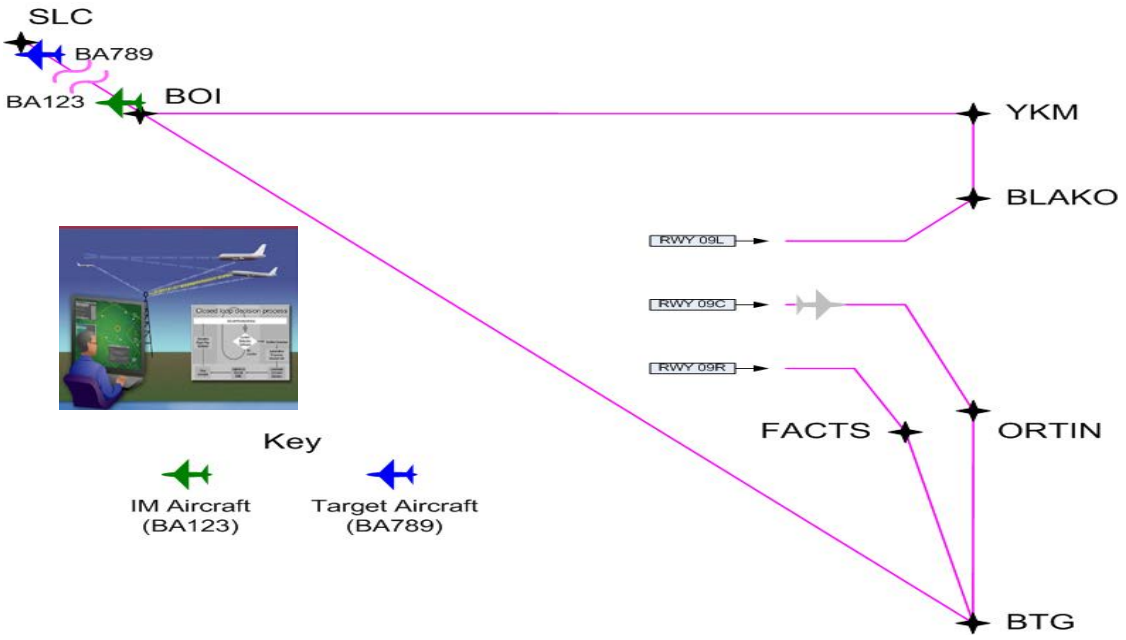


Figure D3. Simple Version of the Scenario (C)

In the maintain mode, the FIM-S system continues to provide speed guidance to the flight crew of BA123 and to the aircraft's automation. Minor changes in speed result from correction of the small spacing error apparent at the achieve-by point (BOI) and from inaccuracies in wind and atmospheric temperature forecasts compared with the values experienced. As the aircraft levels at its assigned cruise altitude, control of speed reverts from use of pitch attitude to modulation of engine thrust.

As BA789 passes SLC with BA123 90.3 seconds behind, the FIM-S system in BA123 terminates the operation. The flight crew of BA123 informs the Center controller of the termination and advises that current speed is 0.826M. The controller clears the crew for use of normal cruise speed and conventional (non-FIM-S) operations resume.

D.2. Complex Version of the Scenario

A more complex and potentially more realistic version of the scenario would see streams of aircraft departing from three runways to form a single stream starting at BOI. There would also be an intermediate merge point at BTG for two of the runway departure streams. In addition, some of the aircraft to be considered would be equipped with neither ADS-B IN (so no FIM-S capability) nor functional ADS-B Out but meeting the terms of the Minimum Equipment List for the flight (so it cannot be a target for FIM-S). Such a scenario would introduce additional complexity to the operations and allow consideration of additional enablers in the ATM domain.

Coordination of takeoffs from the three runways would have to take into account the following:

- Taxi route length, complexity, and intersections/merges with other taxi streams
- The need to deliver aircraft to the right runway ends in the right order at appropriate times
- Provision of takeoff clearances at times consistent with the different path lengths to the merge points including allocation of time-based takeoff 'brackets' that allow the crew to respond to the FIM-S system's guidance on departure intervals
- Aircraft performance characteristics including plans for takeoff and climb thrust derates extracted from the flight plan.

To satisfy all requirements, the ground and tower controllers utilize an airport surface traffic management tool and good communication between controllers, perhaps through some combination of voice and data communication. This tool would also coordinate/be integrated with the integrated arrival/departure manager.

Since each aircraft in the stream (assuming all are FIM-S-equipped) is instructed to achieve the assigned spacing goal by BOI, minor differences in lift-off time and differences in aircraft climb performance compared with those assumed might result in traffic conflicts during the merge at BTG. In order to assure separation at BTG, the departure manager function (part human and part decision support tool) would need to be integrated in its operation with the airport surface traffic management tool and strong coordination would be necessary between tower and approach (departure) controller. Figure D4 illustrates the traffic stream. All aircraft are depicted as FIM-S-equipped and each has been assigned an interval of 90 seconds from the preceding aircraft. All aircraft between BOI and SLC have already achieved the assigned spacing and are maintaining that spacing value. Aircraft between YKM and BOI and between BTG and BOI have been assigned the spacing, but variations in spacing occasioned by takeoff time variance and by the need to provide separation between merging streams at BTG has resulted in a need to adjust the interval to achieve the assigned value. As is apparent from the diagram, an aircraft's preceding aircraft at BOI is likely to have taken off from a different runway.

Although not the case in the illustration above, not all aircraft in the stream may be equipped to conduct FIM-S operations; some of them may not even have ADS-B Out functionality of sufficient quality to support FIM-S as targets. In such a case, to maximize use of FIM-S by not starting a new string of FIM-S operations each time there is an unequipped aircraft in the stream, the controller can instruct a FIM-S-equipped aircraft to space on an aircraft two or three ahead in the final, single stream. Assuming that the target aircraft remains within ADS-B range, this operation is no different for the crew of the FIM-S aircraft than the simple operation described above. However, the controller must now keep the unequipped aircraft close to the center of the gap between the FIM-S target aircraft ahead and the FIM-S aircraft behind, and do

so as these two aircraft adjust speed to meet their spacing assignments (the target aircraft may be a FIM-S aircraft spacing on another aircraft ahead). In order to reduce controller workload, ATM ground system automation would need to provide speed guidance for the unequipped aircraft (part of a future GIM-S function). Since aircraft cross into Center airspace during the operation, coordination between the airport approach controller and the Center controller must ensure that the nature of the overall operation (FIM-S with mixed equipage and some aircraft requiring speed guidance) is understood at handoff. If the controller fails to provide speed instructions that keep the aircraft adequately spaced, the aircraft ahead of or behind the unequipped aircraft might experience a TCAS Resolution Advisory which would introduce a significant perturbation into the flow. It is clear, therefore, that the controller must understand when an RA might be triggered.

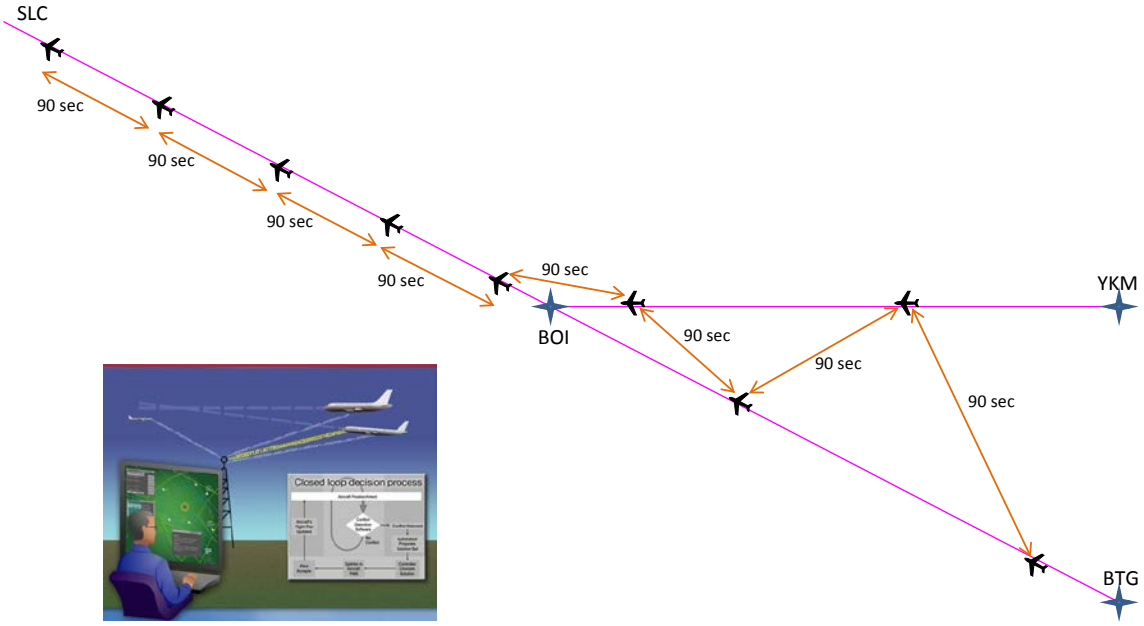


Figure D4. Complex Version of the Scenario

If wind and temperature data predictions are sufficiently inaccurate (e.g., position of a frontal zone is not as predicted), FIM-S aircraft will adjust speed more frequently and perhaps by greater amounts than would otherwise be the case, increasing flight crew workload to a degree. Such variations might create string instability with spacing varying in an oscillatory manner and more significantly the further back down the string of aircraft. If control of unequipped aircraft is also included, use of different weather predictions, of different support tool algorithms than in the aircraft, and of different control loop lengths, controller-to-pilot vs. FIM-S system-to-pilot might result in larger and/or more aggressive speed changes that might add to the instability. The FIM-S algorithm may limit the size and rate of speed changes to contain such instability while the controller might minimize the number (but in doing so increase the size) of speed changes to contain workload.

Any disturbance to the flow might trigger similar effects. Examples might include: the need to instruct an aircraft toward the head of the stream to fly level for conflict resolution would result in similar needs for trailing aircraft and differences in observed target groundspeeds compared with predictions; speed instructions for conflict resolution to a target aircraft perhaps following

handoff to Center and owing to poor coordination; a target aircraft reducing speed to turbulence penetration speed when it encounters convective weather.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01- 02 - 2013	Contractor Report	03-14-2012 - 12-13-2012

4. TITLE AND SUBTITLE

Safety Sufficiency for NextGen: Assessment of Selected Existing Safety Methods, Tools, Processes, and Regulations

5a. CONTRACT NUMBER

NNL06AA04B

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Xu, Xidong; Ulrey, Mike L.; Brown, John A.; Mast, Jim; Lapis, Mary B.

5d. PROJECT NUMBER

5e. TASK NUMBER

NNL12AB38T

5f. WORK UNIT NUMBER

534723.02.02.07.10

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

NASA Langley Research Center
Hampton, Virginia 23681

Boeing Research & Technology
P.O. Box 3707 MC 8R-79
Seattle, WA 98124-2207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSOR/MONITOR'S ACRONYM(S)

NASA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

NASA/CR-2013-217801

12. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified - Unlimited
Subject Category 03
Availability: NASA CASI (443) 757-5802

13. SUPPLEMENTARY NOTES

Langley Technical Monitor: C. Michael Holloway

14. ABSTRACT

NextGen is a complex socio-technical system and, in many ways, it is expected to be more complex than the current system. It is vital to assess the safety impact of the NextGen elements (technologies, systems, and procedures) in a rigorous and systematic way and to ensure that they do not compromise safety. In this study, the NextGen elements in the form of Operational Improvements (OIs), Enablers, Research Activities, Development Activities, and Policy Issues were identified. The overall hazard situation in NextGen was outlined; a high-level hazard analysis was conducted with respect to multiple elements in a representative NextGen OI known as OI-0349 (Automation Support for Separation Management); and the hazards resulting from the highly dynamic complexity involved in an OI-0349 scenario were illustrated. A selected but representative set of the existing safety methods, tools, processes, and regulations was then reviewed and analyzed regarding whether they are sufficient to assess safety in the elements of that OI and ensure that safety will not be compromised and whether they might incur intolerably high costs.

15. SUBJECT TERMS

Costs; Dynamic complexity; Hazards; NextGen; NextGen elements; Safety methods; Safety processes; Safety regulations; Safety tools

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			STI Help Desk (email: help@sti.nasa.gov)
					19b. TELEPHONE NUMBER *(Include area code)*
U	U	U	UU	80	(443) 757-5802